Junos DDoS Secure CLI User Manual

Published: 2013-07-25

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Copyright © 2013, Juniper Networks, Inc.

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company.Copyright©1986-1997,Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979,1980,1983,1986,1988,1989,1991,1992,1993,1994.The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on KirtonsEGP, UC Berkeleys routing daemon (routed), and DCNs HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996,1997, Maker Communications, Inc.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of the respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document .Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

DATA LICENSE (GeoLite Country and GeoLite City databases)

Copyright (c) 2008 MaxMind, Inc. All Rights Reserved.

All advertising materials and documentation mentioning features or use of this database must display the following acknowledgment: "This product includes GeoLite data created by MaxMind, available from http://maxmind.com/"

Redistribution and use with or without modification, are permitted provided that the following conditions are met:
1. Redistributions must retain the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

2. All advertising materials and documentation mentioning features or use of this database must display the following acknowledgement:
"This product includes GeoLite data created by MaxMind, available from http://maxmind.com/"

3. "MaxMind" may not be used to endorse or promote products derived from this database without specific prior written permission.

THIS DATABASE IS PROVIDED BY MAXMIND, INC ``AS IS AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL MAXMIND BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS DATABASE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Some parts of this software distribution are derived from the APNIC, ARIN and RIPE databases (copyright details below). The author of this module makes no claims of ownership on those parts.

APNIC conditions of use:

The files are freely available for download and use on the condition that APNIC will not be held responsible for any loss or damage arising from the application of the information contained in these reports. APNIC endeavours to the best of its ability to ensure the accuracy of these reports; however, APNIC makes no guarantee in this regard.

In particular, it should be noted that these reports seek to indicate the country where resources were first allocated or assigned. It is not intended that these reports be considered as an authoritative statement of the location in which any specific resource may currently be in use.

ARIN database copyright:

Copyright (c) American Registry for Internet Numbers. All rights reserved.

RIPE database copyright:

The information in the RIPE Database is available to the public for agreed Internet operation purposes, but is under copyright. The copyright statement is: "Except for agreed Internet operational purposes, no part of this publication
may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without prior permission of the RIPE NCC on behalf of the copyright holders. Any use of this
material to target advertising or similar activities is explicitly forbidden and may be prosecuted. The RIPE NCC requests to be notified of any such activities or suspicions thereof.
Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos.5,473,599,5,905,725,5,909,440,6,192,051,6,333,650,6,359,479,6,406,312,
6,429,706,6,459,579,6,493,347,6,538,518,6,538,899,6,552,918,6,567,902,6,578,186, and6,590,785.

Copyright © 2013 Juniper Networks, Inc. All rights reserved. Printed in USA.

Junos DDOS Secure CLI User Manual

Revision History

July 2013

The information in this document is current as of the date listed in the revision history.

SOFTWARE LICENSE

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Website at www.juniper.net/techpubs.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA

Copyright © 2013, Juniper Networks, Inc

Table of Contents

Junos DDoS Secure CLI User Manual i
Objective vi
Audience vi
DDoS Documentation and Release Notes vi
Obtaining Documentation vi
Documentation Feedback vi
Requesting Technical Support vii
Self-Help Online Tools and Resources vii
Opening a Case with JTAC vii
- Serial Port Connection 1
- SSH Connection 1
- System Console Connection 1
- Starting a CLI session 2
- Navigating the CLI 3
- Making Configuration Changes via the CLI 4
- Usage 8
- Portals 9
- User Management 11
- External Authenticators 13
- Access Control 14
- Network Configuration 15
- MAC Gateway Configuration 19
- Appliance Mode Configuration 21
- Shares Configuration 23
- Portal Operational Mode Configuration 24
- Bandwidth and Port Filter Configuration 25
- Filter Aggregation Configuration 29
- Protected IP Configuration 31
- Portal Defense Configuration 34
- Block Country and IPs Configuration 35
- Country Code (geoip) Definitions 36
- Preferred Clients and White-Listing Configuration 38
- Layer 7 Inspection 41
- Disable RFC testing 42
- TCP State Timeouts 43
- CHARM Tuneables 44

Copyright © 2013, Juniper Networks, Inc

Date and Time 45
Remote Alerts, Reports and Logging 47
NetFlow 50
Mail Reporting 51
Logging Thresholds 53
Debug Options 58
Traffic Interception 59
Chassis Definitions 60
System Commands 63
Terminal Configuration 65
how terminal 65
set terminal 65
stats view 67
show version 67
DDoS Secure appliance BGP Configuration 70
Peering Router Sample Configuration 71
Re-Routing Trigger 71
Force Specific Re-Routing 72
Before Configuration 73
After Configuration 73
Content Presentation Information 73
File Naming 73
File Content 73
Intercept Server Information 74
DDoS Secure appliance Engine Configuration 74
Testing 75
Country Block Bypass 75
Sorted by Code 85
Sorted by Country 87
DDoS Secure1200-FAILSAFE Panels 89
Login Page 92
Images / CSS files 92
Updating Customized Files 92
Removing Customized Files 92

Copyright © 2013, Juniper Networks, Inc

ABOUT THIS GUIDE

Objective

The guide provides the command line interface information for the Junos DDoS Secure appliance.

Audience

This guide is designed for network administrators who are installing and maintaining a Junos DDoS Secure appliance. To use this guide, you need a broad understanding of networks in general and the Internet in particular, networking principles, network configuration and virtualization. Any detailed discussion of these concepts is beyond the scope of this guide.

DDoS Documentation and Release Notes

For a list of related DDoS Secure appliance documentation, see is http://www.juniper.net/techpubs/en_US/release-independent/ddos/information-products/pathway-pages/product/index.html

If the information in the latest Junos DDoS Secure appliance Release Notes differs from the information in the documentation, follow the Junos DDoS Secure appliance Release Notes.

Obtaining Documentation

To obtain the most current version of all Juniper Networks technical documentation,see the products documentation page on the Juniper Networks website at http://www.juniper.net/techpubs.

To order printed copies of this guide and other Juniper Networks technical documents, or to order a documentation CD, which contains this guide, contact your sales representative.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback format http://www.juniper.net/techpubs/docbug/docbugreport.html. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version

Copyright © 2013, Juniper Networks, Inc

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are under warranty, and need post sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at http://www.juniper.net/support/requesting-support.html

Copyright © 2013, Juniper Networks, Inc

CHAPTER 1

COMMAND LINE OVERVIEW

The Command Line Interface (CLI), provides a simple command syntax for the purpose of making configuration changes to a DDoS secure appliance. The CLI can be accessed one of three ways:

- ANSI terminal software via a serial line connection to the DDoS secure appliance serial port
- SSH connection to the DDoS secure appliance management interface
- System console with the use of a keyboard and monitor

Serial Port Connection

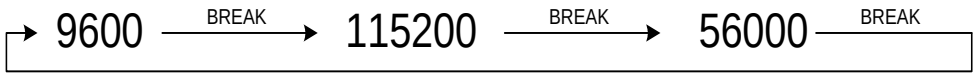
The serial port is located on the back of the DDoS secure appliance and uses industry standard pin outs as shown in the appendix B.

In order to communicate with the DDoS secure appliance, the serial port on the device it is connected to should be set to one of the following settings.

- 9600 baud, 1 stop bit, no parity, and hardware flow control
- 57600 baud, 1 stop bit no parity, and hardware flow control
- 115200 baud, 1 stop bit, no parity, and hardware flow control

The DDoS secure appliance outputs its hardware initialization and booting diagnostic messages at 9600 baud, so this is the recommended speed to use for troubleshooting.

To switch to a faster speed for normal system management, it is necessary to send a BREAK to switch to the next available speed, followed by two or three RETURN or LINE-FEED characters. Each time a BREAK is sent the speed cycles between the supported speeds in the following order:



SSH Connection

In order to use the CLI via the Internet SSH protocol the DDoS secure appliance management interface must first be configured with an appropriate IP Address, Network Mask, Default Gateway and Interface Speed. Secondly, SSH access from the client IP address must be enabled. Both operations are fully documented in the GUI User Manual, and once enabled, can be modified through the CLI.

System Console Connection

The system console itself operates just like a PC with support for a USB or PS2 style keyboard and SVGA monitor.

Copyright © 2013, Juniper Networks, Inc

Starting a CLI session

To start a CLI session, you will need to authenticate to the CLI subsystem via one of the methods described above. The initial default user is **user** and the default password is **password**. It is recommended that these defaults be changed as soon as possible.

Example login via console/serial interface:

```
DDoS secure appliance version 5.13.1.2
ws_192_168_0_196 login: user
Password: password
JS>sh version
DDoS Secure Code Version:      5.13.1-2
DDoS Secure Code Base:         CENTOS_6_3
DDoS Secure Build Date:        201305201820GMT
CD Base Image:                 5.13.1-2
Actual Memory Size:            31.3G
Actual Number of CPUs:         16
Serial No:                     A1RYMW1
Hardware ID:                   90:B1:1C:2A:A3:28
Platform:                      J-DDOS-SEC-AP2
Last Restart:                  Tue May 21 16:54:09 2013
Licensed Throughput:           10G
Memory To Use:                 31G
CPUs To Use:                   16
Protected IPs Supported:       64K
Tracked IPs Supported:         32M
Portals Supported:             256
Filters Supported:             4K
MAC Entries Supported:         16K
TCP Entries Supported:         4M
UDP Entries Supported:         512K
ICMP Entries Supported:        64K
Other IP Entries Supported:    64K
Fragment Entries Supported:    32K
FTP Entries Supported:         8K
JS>
```

Example login via SSH from Unix command line:

```
Prompt> ssh -l user 192.168.0.196
user@192.168.0.196s password: password
JS>sh version
DDoS Secure Code Version:      5.13.1-2
DDoS Secure Code Base:         CENTOS_6_3
DDoS Secure Build Date:        201305201820GMT
CD Base Image:                 5.13.1-2
Actual Memory Size:            31.3G
Actual Number of CPUs:         16
Serial No:                     A1RYMW1
Hardware ID:                   90:B1:1C:2A:A3:28
Platform:                      J-DDOS-SEC-AP2
Last Restart:                  Tue May 21 16:54:09 2013
Licensed Throughput:           10G
Memory To Use:                 31G
CPUs To Use:                   16
Protected IPs Supported:       64K
Tracked IPs Supported:         32M
Portals Supported:             256
```


Copyright © 2013, Juniper Networks, Inc

```
Filters Supported:              4K
MAC Entries Supported:          16K
TCP Entries Supported:          4M
UDP Entries Supported:          512K
ICMP Entries Supported:         64K
Other IP Entries Supported:     64K
Fragment Entries Supported:     32K
FTP Entries Supported:          8K
JS>
```

As described in the GUI User Manual, users are allocated to different Portals (virtual DDoS secure sub-appliance) and any user access to the CLI will only allow configuration of their Portal. If the Portal is anything other than the master Portal (webscreen), then this is indicated in the prompt as follows:

```
Prompt> ssh –l portaluser 192.168.0.196
user@192.168.0.196s password: password
JS portal>show config
version e2
configuration portal
remove user all
remove server all
remove fagg all
remove filter all
set operation mode defensive countries all aslist all
set user portaluser password $1$blI73sjE$wA.A7vHC1qvdfROlEHJtM. perms administrator
...
set mail server none dailystats yes alerts no
JS portal>
```

Navigating the CLI

The CLI environment has shortcuts and built in help messages to aid in the configuration of the appliance.

When entering a command or the name of a parameter, it is not necessary to type the full name. A command may be abbreviated to the smallest sequence of characters that uniquely identify the command.

- Pressing the TAB key will attempt to automatically complete the current command being entered. If the command could not be completed then pressing the TAB key again displays a brief list of available matching commands. Once a command has been entered, TAB will complete the next parameter, or if there is more than one option it will list the available parameters that are valid.
- Pressing the up and down cursor keys cycles through the previously entered commands.
- The left and right cursor keys can be used to move back and forth along the text line currently displayed; enabling any part of the line to be re-edited before it is submitted.

When displaying information in which the text to be displayed is longer than a single screen, the output is paused and the phrase—more—is shown on the bottom of the screen. Pressing [SPACE] displays the next page of information, [ENTER] displays the next line, and [Q] will exit the display process and the CLI will return to the previous command prompt state.

If the CLI commands are scripted, issuing the `set terminal pause off` command will turn off the terminal pause. This setting is not remembered across sessions and therefore

Copyright © 2013, Juniper Networks, Inc

will need to be entered at the start of every CLI session if required. Terminal pause can be enabled again by issuing the `set terminal pause on` command.

Making Configuration Changes via the CLI

The CLI has three principle commands for operating on the configuration: `show`, `set`, and `remove`.

- `show`: This is a general-purpose command used to display the current value for various configuration settings. Changes to these configuration settings are performed via the set and remove commands.
- `set`: This command is used in the majority of cases to configure the system.
- `remove`: This command is used to completely remove a block of configuration (a table entry), such as a server and all its settings. Most individual settings, however, cannot be removed as they must have a value. Such settings can only be changed from one value to another with the set command.

When making changes to the configuration via the CLI, the pending changes are recorded and applied later when instructed by the operator. At any time prior to applying the new configuration the list of changes to be made can be displayed or cleared.

When the first configuration line is entered, a snapshot of the current configuration is made and all subsequent configuration changes are made against the snapshot configuration. The `apply` command takes the snapshot configuration, applies the configuration changes to it, and then activates the new configuration. This method avoids the possibility of other people changing the configuration at the same time in such a way that your configuration cannot be applied.

Warning: If two people change the configuration simultaneously then the last person to apply gets their changes made and the other person loses their changes. For this reason warnings are given when two people start to change the configuration at the same time.

Any command used to change the configuration may have the `now` keyword at the end of the input line which causes that configuration change to be applied immediately.

NOTE: `now` keyword cannot be used when there are any pending changes yet to be applied.

All CLI commands are case sensitive and must be entered in lower case. Most parameters are also case sensitive with exceptions detailed in the individual sections contained within this document.

apply

The `apply` command commits and invokes any pending configuration changes.

write

The `write` command commits and invokes any pending configuration changes

Copyright © 2013, Juniper Networks, Inc

discard

It is often helpful when a large amount of configuration has been performed and an error detected, to issue the `show pending changes` command prior to `discard`. Then relevant parts of the previous configuration changes can simply be copied back into the terminal. If another person has started editing the configuration, you can also use this method to show the configuration changes you have made. Once the other person has finished, you can then issue the discard button, paste back in your changes, then apply. This procedure will avoid undoing the other user changes.

revert

The `revert` command reverts the DDoS secure appliance appliance back to the previous configuration.

The previous configuration is defined as the configuration prior to the last committed configuration change (with `apply`, or the command suffixed with `now`).

Warning: A `revert` may also undo any configuration changes performed by other users, therefore care should be taken when using this command.

now

The `now` command is not a command in its own right. Instead, it is an option that can be appended as the last argument to any CLI command used to change the configuration. When used, the appended command is not added to the list of pending changes but is executed immediately, changing the current running configuration. The `now` option cannot be used if there are any pending changes waiting to be applied. Any such pending changes must either be applied or discarded (see `apply` and `discard`) before a command can use the `now` option.

show config

Synopsis: `show` config

The `show config` command displays the device current active configuration.

Example:

```
JS>show config
…
set mail server none
set access https all
set access ssh all
set access snmp 192.168.1.221
```

show run

Synopsis: show run

The show run command displays the device current active configuration.

Example:

```
JS>show run
…
set mail server none
set access https all
set access ssh all
```

Copyright © 2013, Juniper Networks, Inc

```
set access snmp 192.168.1.221
```

show pending changes

Synopsis: show pending changes

The show pending changes command displays the list of pending changes for the current user session. The pending changes of other CLI users will not be displayed.

Example:

```
JS>set access https 192.168.0.0/16
JS>set access ssh 192.168.0.0/16
JS>set access snmp 192.168.0.0/16
JS>show pending changes
set access https 192.168.0.0/16
set access ssh 192.168.0.0/16
set access snmp 192.168.0.0/16
JS>
```

exit

The `exit` command exits from the CLI.

quit

The `quit` command exits from the CLI.

context

Synopsis: context newportal

The context command allows a user to change between Portals, but only if originally logged into the DDoS secure appliance Portal.

Copyright © 2013, Juniper Networks, Inc

Copyright © 2013, Juniper Networks, Inc

CHAPTER 2

CONFIGURATIONS

This chapter helps you to configure the setting in a DDoS Secure appliance.

Usage

It is possible to define different table sizes for all the tracked information. The defined sizes are subject the amount of RAM, so the DDoS Secure appliance will reduce or or more of the values if they are too large.

The following describes the usage parameters and their formats.

Table 1: Portal Parameters

PARAMETER	VALUE	DESCRIPTION
hwid	HARDWARE-ID	The hardware ID of the appliance
bandwidth	1G|2G|3G|4G|5G|6G|7G|8G|9G|10G	The size of the purchased License.
memory	[1-65536[MG]]	The amount of RAM to use
cpus	1|2|3|4|6|8|12|16	The number of CPUs to use
protected	2|4|8|16|32|64|128|256|512|1K|2K|4K|8K|16K|32K|64K	The number of protected IPs
portals	2|4|8|16|32|64|128|256	The number of protected IPs
tracked	128K|256K|512K|1M|2M|4M|8M|16M|32M	The number of tracked IPs
macs	128|256|512|1K|2K|4K|8K|16K|32K	The number of MAC addresses
tcps	128K|256K|512K|1M|2M|4M	The number of TCP sessions
udps	128K|256K|512K|1M|2M|4M	The number of UDP sessions
icmps	2K|4K|8K|16K|32K|64K	The number of ICMP sessions
others	2K|4K|8K|16K|32K|64K	The number of Other IP sessions
frags	2K|4K|8K|16K|32K	The number of Fragment Sessions
ftps	512|1K|2K|4K|8K|16K	The number of FTP Sessions

Copyright © 2013, Juniper Networks, Inc

show usage

Synopsis:

`show usage`

Description

Displays the usage settings.

Example:

```
JS>show usage
set usage hwid 90:B1:1C:2A:A3:28 bandwidth 10G cpus 16 memory 31G protected 64K portals 256 \
       filters 4K macs 16K tracked 32M tcps 4M udps 512K icmps 64K others 64K frags 32K \
       ftps 8K
```

set usage

Synopsis: `set usage [hwid HWID] \`
`[bandwidth <1G|2G|3G|4G|5G|6G|7G|8G|9G|10G>] \`
`[memory <[1-65536[MG]]>] \`
`[cpus <1|2|3|4|6|8|12|16>] \`
`[protected <2|4|8|16|32|64|128|256|512|1K|2K|4K|8K|16K|32K|64K>] \`
`[portals <2|4|8|16|32|64|128|256>] \`
`[tracked <128K|256K|512K|1M|2M|4M|8M|16M|32M>] \`
`[macs <128|256|512|1K|2K|4K|8K|16K|32K>] \`
`[tcps <128K|256K|512K|1M|2M|4M>] \`
`[udps <128K|256K|512K|1M|2M|4M>] \`
`[icmps <2K|4K|8K|16K|32K|64K>] \`
`[others <2K|4K|8K|16K|32K|64K>] \`
`[frags <2K|4K|8K|16K|32K>] \`
`[ftps <512|1K|2K|4K|8K|16K>]`

The `set usage` command can be used to update the usage tables.

Portals

It is possible to specify blocks of addresses (networks and or single IP addresses)–known as Portals, which can be managed separately by designated users. This gives the ability for customers, clients or Business Groups to be able to manage what DDoS secure appliance does for their Portal. Any user that has full managerial access can override these Portal configurations. The master Portal is known as DDoS secure appliance.

The sum of all the values of the Portals (excluding the Master) cannot exceed that of the Master Portal, with the exception of the Burst values, which individually cannot exceed that of the Master Portal.

The following describes the portal parameters and their formats.

Table 2: Portal Parameters

PARAMETER	VALUE	DESCRIPTION
ip	IPRANGE|all	The list of protected IP addresses.
Vlan	VLANSDEF	The list of Vlans / MPLS definitions to track as opposed to IP addresses.
validpkts	PKTS|U	Guaranteed packet rate.

Copyright © 2013, Juniper Networks, Inc

burstpkts	PKTS|U	Burstable packet rate. Over this rate triggers an Incident.
validspeed	SPEED|U	Guaranteed bandwidth.
burstspeed	SPEED|U	Burstable bandwidth. Over this rate triggers an Incident.
Filters	FILTERS	The number of configurable filters.
Rerouteminpkts	PKTS	ReRouting is dropped when IP is below this packet rate.
Reroutemaxpkts	PKTS	ReRouting is potentially triggered when above this packet rate.
Rerouteminspeed	SPEED	ReRouting is dropped when IP is below this bandwidth.
Reroutemaxspeed	SPEED	ReRouting is potentially triggered when above this bandwidth.
Protected	PROTECTED	The number of configurable protected IP addresses.

show portal

Synopsis:

`show portal <PORTALNAME|all>`

Description

Displays the settings of the named portal.

Example:

```
JS>show portal test1
set portal test1 ip 10.0.0.0/24 validpkts 3720 burstpkts 3720 validspeed 10M \
       burstspeed 50M filters 31 rerouteminpkts 1K reroutemaxpkts 50K rerouteminspeed 20M \
       reroutemaxspeed 1G protected 16
```

Alternatively the reserved portal name `all` can be specified to show all defined portals.

Example:

```
JS>show portal all
set portal DDoS secure appliance ip all validpkts 37.2K burstpkts 37.2K validspeed 100M \
       burstspeed 100M filters 991 rerouteminpkts 1K reroutemaxpkts 50K rerouteminspeed \
       20M reroutemaxspeed 1G protected 1
set portal example ip 10.0.0.0/24 validpkts 3720 burstpkts 3720 validspeed 10M \
       burstspeed 50M filters 31 rerouteminpkts 1K reroutemaxpkts 50K rerouteminspeed 20M \
       reroutemaxspeed 1G protected 16
```

remove portal

Synopsis: `remove portal <PORTALNAME|all>`

This command can be used to delete a specific portal.

This command can also be used to delete all current portals. To do this the parameter value all is used instead of a portal name. When deleting all portals the command will ask for confirmation.

NOTE: It is possible to disable the prompting, which can be useful for automated scripts; see `set terminal confirmations`.

Copyright © 2013, Juniper Networks, Inc

set portal

Synopsis: `set portal <PORTALNAME> [ip <IPRANGE|all>|vlan <VLANSDEF>] \`
`[validpkts <PKTS>] [burstpkts <PKTS>] \`
`[validspeed <SPEED>] [burstspeed <SPEED>] \`
`[filters <FILTERS>] [rerouteminpkts <PKTS>] \`
`[reroutemaxpkts <PKTS>] [rerouteminspeed <SPEEED>] \`
`[reroutemaxspeed <SPEEED>] [protected <PROTECTED>]`

The `set portal` command can be used to create a new portal or modify an existing one.

User Management

There are four types of user accounts as determined by one of the following permissions. Users are only allowed to access their allocated Portal information.

Table 3: User Access Permissions

PARAMETER	VALUE
administrator	User has full access to change any configuration entry.
operator	User has full access to change any configuration entry other than user account configuration. Limited read-only access to user information.
guest	User has read-only access to configuration settings. User has no access to user information.
sso	User can only change user information.

The following tables describe the User parameters and their formats.

Table 4: User Account Parameters

PARAMETER	VALUE	DESCRIPTION
User	USERNAME	The username for this account
password	PASSWORD	The user password.
Perms	PERMS	The user access permissions.

show user

Synopsis: `show user <USERNAME|all>`

The full list of the configured user accounts can be shown by issuing the command show user all. If the user issuing the command has administrator or sso permissions then the encrypted passwords are also shown along with the account name and permissions.

Example:

```
JS>show user all
set user user password $1$ehL5yai/$ewwyx00qx3VIdKXITvRUG. perms administrator
set user test password $1$wLh6yBh0$vmth1CmyrvQDg6ZKDTuqn. perms operator
```

Copyright © 2013, Juniper Networks, Inc

Users with `operator` permissions will be shown the list of users without the passwords.

Example:

```
JS>show user all
set user user perms administrator
set user test perms operator
```

Alternatively, the details of a specific user can be shown if the user username is specified instead of the parameter all.

This command is not available to guest accounts.

Example:

```
JS>show user test
set user test password $1$wLh6yBh0$vmth1CmyrvQDg6ZKDTuqn. perms operator
```

remove user

Synopsis: `remove user <USERNAME|all>`

This command can be used to delete a specific user. Only administrators can remove users, and they cannot delete themselves or change their own permission status.

This command can also be used to delete all current users. To do this the parameter value all is used instead of a user account name. Administrators can use remove user all but the command will not remove the administrator user account used to issue it. When deleting all users the command will ask for confirmation.

NOTE: It is possible to disable the prompting, which can be useful for automated scripts; see set terminal confirmations.

set user

Synopsis: `set user <USERNAME> [password <PASSWORD>] \ [perms <administrator|operator|guest|sso>]`

The `set user` command can be used to create a new user or modify an existing one.

When creating a new user the password must be specified. If the permissions are not specified then perms guest is assumed.

For an existing user account the set user command can be used to modify either the password, or the permissions, or both.

When specifying the password either the encrypted form or a plain text password may be entered. An encrypted password, in the form of an MD5 hashed key, is recognized by the password starting with 1.

NOTE: There is no echo suppression or masquerading of the input data when using the set user command, even when plain text password entry is in use.

Warning: Unlike the Web-based interface, there is no prompting for a repeat of the password entry, therefore extra care must be taken to avoid typing mistakes.

Copyright © 2013, Juniper Networks, Inc

External Authenticators

There are two types of external authenticators, as well as the local password file for authentication. If an external authenticator is defined and enabled, then the password checking order is external (radius), then external (TACACS+), if that fails then local.

Table 5: External Authenticator Types

PARAMETER	VALUE	DESCRIPTION
radius	Requires an external Radius server which holds the user authentication records.	Radius
tacacs+	Requires an external Tacacs+ server which holds the user authentication records.	TACACS+

NOTE: TACACS+ is not available by default.

The following tables describe the External Authenticator parameters and their formats.

Table 6: External Authenticator parameters

PARAMETER	VALUE	DESCRIPTION
server	IPADDRESS	The IP address of the server.
backup	IPADDRESS|none	Alternative server IP address.
becret	SECRET	The secret need to encrypt / decrypt the authentication session
enabled	yes|no	Whether the authenticator is enabled or not.
port	PORT	The port the Radius server is listening on.
protocol	TPROTOCOL	TACACS+ protocol.
service	TSERVICE	TACACS+ service.

show auth

Synopsis: `show auth`

The full list of the authenticator definitions are shown.

Example:

```
JS>show auth
set auth radius server 192.168.0.3 backup none port 1812 secret secret enabled yes
set auth tacacs+ server 192.168.0.3 backup none secret secret-1 protocol lcp service \
   DDoS secure appliance enabled no
```

Users with operator permissions will be shown the secrets masked out.

Example:

```
JS>show auth
set auth radius server 192.168.0.3 backup none port 1812 secret xxxxxxxx enabled yes
```

Copyright © 2013, Juniper Networks, Inc

```
set auth tacacs+ server 192.168.0.3 backup none secret xxxxxxxx protocol lcp service \
   juniper enabled no
```

set auth

Synopsis: `set auth radius server <IPADDRESS> \`
`[backup <IPADDRESS>|none> secret <SECRET> [port <PORT>]`

`set auth tacacs+ server <IPADDRESS> \`
`[backup <IPADDRESS>|none>] secret <SECRET>`
`protocol <TPROTOCOL> service <TSERVICE>`

The `set auth` command can be used to modify any parameters of an Authenticator definition.

A user has to be defined on the DDoS secure appliance (with a password) before it can be used to either connect to the GUI, or connect via SSH. It is recommended that there is at least one known local password so that it is possible to authenticate to the DDoS secure appliance in an emergency should the external authenticator not be available.

Access Control

DDoS secure appliance supports multiple remote access methods. The control of each type of access must be specified with its own `set access` command. The following are the different access types.

NOTE: Only IPv4 addresses are currently supported.

Table 7: Access Types

ACCESS	DESCRIPTION
ssh	Specified IP addresses can access the CLI via SSH.
https	Specified IP addresses can access the Web-based interface.
snmp	Specified IP addresses are able to read the DDoS secure appliance SNMP tables.
https_juniper	DDoS secure appliance defined Juniper Networks public IPs are allowed access if enabled.
ssh_juniper	DDoS secure appliance defined Juniper Networks public IPs are allowed access if enabled.

When configuring access control, DDoS secure appliance considers IP addresses and their networks as classless. Both IP host addresses and IP network addresses can be used. A network address can be specified in either network/mask or network/bits format. The table below illustrates the various supported formats.

A compound value is parsed as a single entry when entered; there can be no spaces between the entries and commas that separate them.

show access

Synopsis: `show access all`

The `show access all` command will list the current access settings.

Example:

Copyright © 2013, Juniper Networks, Inc

```
JS>show access all
set access https 192.168.1.0/24,192.168.2.3
set access https_juniper yes
set access ssh all
set access ssh_juniper yes
set access snmp 192.168.1.1
```

It is also possible to show individual values by specifying the access type of interest.

Example:

```
JS>show access https
set access https 192.168.0.0/16
set access https_juniper yes
```

set access https

Synopsis: `set access https <IPGROUP|all|none>`

This command sets the list of IP addresses permitted to connect to the Web-based configuration interface.

set access https_DDoS secure appliance

Synopsis: `set access https_DDoS secure appliance <yes|no>`

This command enables / disables the DDoS secure appliance defined list of DDoS secure appliance public IP addresses permitted to connect to the Web-based configuration interface.

set access ssh

Synopsis: `set access ssh <IPGROUP|all|none>`

This command sets the list of IP addresses permitted to connect via SSH to the command line configuration interface.

NOTE: The IP address of the client issuing the command via an SSH connection cannot be removed from the access list. This avoids the possibility of a user locking themselves out. If it is wished that SSH access is to be totally disabled, then this can be done via the CLI over the serial interface or via the Web-based configuration interface.

set access ssh_DDoS secure appliance

Synopsis: `set access ssh_DDoS secure appliance <yes|no>`

This command enables / disables the DDoS secure appliance defined list of DDoS secure appliance public IP addresses permitted to connect to the CLI configuration interface.

set access snmp

Synopsis: `set access snmp <IPGROUP|all|none>`

This command sets the list of IP addresses permitted to connect to the SNMP management interface for MIB browsing.

Network Configuration

Each DDoS secure appliance has four network interfaces, along with a common definition:

Copyright © 2013, Juniper Networks, Inc

Table 8: Interface types

INTERFACE NAME	DESCRIPTION
Management	The Management interface, for DDoS secure appliance management.
Protected	The protected interface, connected to the protected hosts on the LAN.
Internet	The Internet interface, connected to hosts on the rest of the LAN or the Internet.
Datashare	The Data Share interface, used to share state and incident information between DDoS secures appliances. This interface may not be available on all hardware configurations.
Global	For setting parameters that are common to both the Internet and protected interfaces.

The following table lists all the possible configuration parameters, however not any interface type will accept them all. IP Addresses can only be configured on the Management and Data Share interfaces as they are the only interfaces on a DDoS secure appliance unit that have an active TCP/IP stack.

Table 9: Interface parameters

PARAMETER	VALUE	DESCRIPTION
hwid	HARDWARE-ID	The Hardware ID of the appliance. If this parameter is specified then any following parameters are ignored if the Hardware ID specified does not match that of the appliance. This parameter is always shown when displaying the configuration because interface configuration is unique to an individual appliance.
IP	IPADDRESS	The IPv4 address of the appliance Management or Data Share interface.
netmask	NETMASK	The netmask of the appliance Management or Data Share interface.
gateway	IPADDRESS|none	The default gateway of the appliance Management interface. Specify none to clear the default gateway.
linkmode	LINKMODE	The link mode of the interface.
Fcmode	FCMODE	The flow control mode of the interface.
Mtu	MTU_SIZE	The MTU size (default 1500) for traffic flowing between the internet and protected interfaces.
Lfpt	<yes|no>	Whether a link failure on one (internet/protected) interface of the DDoS secure appliance is to be passed through to the other side by dropping the transmitter.
Cdp	<yes|no>	Whether all the interfaces are to generate CDP packets or not.

Copyright © 2013, Juniper Networks, Inc

trackvlans	<yes|no>	If set, different vlans will cause different stateful sessions even if they have the same IPs and ports.

show interface

Synopsis: `show interface all`

This command displays the network interface configuration. Each interface can be configured with or without the unique appliance Hardware ID (always shown on display output), which enables the automatic generation of a common configuration to be shared with multiple DDoS secure appliance units, while also allowing each unit to have customized network interface configurations when the Hardware ID is included.

Example:

```
JS>show interface all
set interface management hwid 00:01:02:03:04:05 ip 192.168.30.30 \
   netmask 255.255.255.0 gateway 192.168.30.1 linkmode auto fcmode full
set interface protected hwid 00:01:02:03:04:05 linkmode auto fcmode none
set interface internet hwid 00:01:02:03:04:05 linkmode auto fcmode none
set interface datashare hwid 00:01:02:03:04:05 ip 10.1.1.30 netmask 255.255.255.0 \
   linkmode auto fcmode none mtu 1500
set interface global mtu 1500 cdp yes lfpt no trackvlans no
```

The configuration of a single interface can be shown by specifying the specific interface of interest.

Example:

```
JS>show interface protected
set interface protected hwid 00:01:02:03:04:05 linkmode auto fcmode none
```

set interface management

Synopsis: `set interface management [hwid <HARDWARE-ID>] \`
`[ip <IPADDRESS>] [netmask <NETMASK>] \`
`[gateway <GATEWAY|none>] [linkmode <LINKMODE>] \`

`[fcmode <FCMODE>]`

This command is used to set the basic TCP/IP configuration and link mode of the Management interface. The TCP/IP options are needed for remote network management of the DDoS secure appliance unit. One or more of the parameters can be configured at the same time, with or without the addition of the `hwid` parameter (but the `hwid` parameter cannot be specified alone). Even if only one parameter is set, all of the current settings are shown when the configuration is displayed.

set interface datashare

Synopsis: `set interface datashare [hwid <HARDWARE-ID>] \`
`[ip <IPADDRESS|none] [netmask <NETMASK>] \`
`[linkmode <LINKMODE>] [fcmode <FCMODE>] [mtu <MTU_SIZE>]`

This command is used to set the basic TCP/IP configuration and link mode of the Data Share interface. If the IP address is set to `none`, then the Data Share interface will not be used. One or more of the parameters can be configured at the same time, with or without the addition of the `hwid` parameter (but the `hwid` parameter cannot be specified alone). Even if only one parameter is set, all of the current settings are shown when the configuration is displayed.

set interface protected

Copyright © 2013, Juniper Networks, Inc

Synopsis: `set interface protected [hwid <HARDWARE-ID>] \ linkmode <LINKMODE> [fcmode <FCMODE>]`

This command sets the link mode of the protected interface. Not all link mode values may be supported depending on the DDoS secure appliance model. The specification of `hwid <HARDWARE-ID>` is optional but helps avoid miss-configuration when sharing configuration files between DDoS secure appliance units. The `hwid` option and its value are always included when the configuration is displayed or saved. The `hwid` option cannot be specified alone.

If this interface spans multiple interfaces (WS-3G), then all sub interfaces will be set to the same specification. Load sharing across the multiple interfaces will be done by the switch connected to the protected interface. Any 802.3ad packets are passed through to the Internet interface for onward transmission so that the Internet and protected switches can set up their own link aggregation. Any packet received on one of the sub interfaces will be sent out of the corresponding sub interface. The upstream / downstream switch must be configured for lag / teaming mode and load share appropriately.

set interface internet

Synopsis: `set interface internet [hwid <HARDWARE-ID>] \ linkmode <LINKMODE> [fcmode <FCMODE>]`

This command sets the link mode of the Internet interface. Not all link mode values may be supported depending on the DDoS secure appliance model. The specification of `hwid <HARDWARE-ID>` is optional but helps avoid mis-configuration when sharing configuration files between DDoS secure appliance units. The `hwid` option and its value are always included when the configuration is displayed or saved. The `hwid` option cannot be specified alone.

If this interface spans multiple interfaces (WS-3G), then all sub interfaces will be set to the same specification. Load sharing across the multiple interfaces will be done by the switch connected to the Internet interface. Any 802.3ad packets are passed through to the protected interface for onward transmission so that the Internet and protected switches can set up their own link aggregation. Any packet received on one of the sub interfaces will be sent out of the corresponding sub interface. The upstream / downstream switch must be configured for lag / teaming mode and load share appropriately.

set interface global

Synopsis: `set interface global mtu <MTU_SIZE> lftp <yes|no> \ cdp <yes|no> trackvlans <yes|no>`

This command sets the common definition for traffic flowing between the internet and protected interfaces, as well as if CDP packets are to be generated or not on all interfaces.

show dns

Synopsis: `show dns`

This command is used to show the current DNS configuration.

Example:

```
JS>show dns
set dns forwarder 192.168.0.3
```

set dns

Synopsis: `set dns forwarder <IPADDRESS>`

This command is used to set the IP address of the DNS server(s) to forward any DNS queries to.

Copyright © 2013, Juniper Networks, Inc

Example:

```
JS>set dns forwarder 192.168.0.3
JS>show dns
set dns forwarder 192.168.0.3
```

remove route

Synopsis: `remove route <all|IPNETWORK>`

This command is used to remove additional routing.

show route

Synopsis: `show route <all|IPNETWORK>`

This command is used to show the additional routing.

Example:

```
JS>show route all
Not configured
```

set route

Synopsis: `set route cidr <IPNETWORK> gateway <IPADDRESS>`

This command is used to set up additional routing incase the default gateway is insufficient for access to different IP addresses. It is not normally required as the default gateway is usually sufficient.

Example:

```
JS>show route all
Not configured
JS>set route cidr 192.168.1.0/24 gateway 192.168.0.1
JS>show route all
Set route cidr 192.168.1.0/24 gateway 192.168.0.1
```

MAC Gateway Configuration

A DDoS secure appliance unit operates at both the Ethernet layer and the internet protocol layers. Defense is managed at the Ethernet layer based on a list of gateways, which are tracked by Ethernet MAC addresses. The Ethernet addresses discovered may be those of routers and firewalls, or they may be those of individual hosts, but they are all treated the same way. Ethernet addresses detected on the DDoS secure appliance internet interface are classed as internet gateways and the addresses detected on the DDoS secure appliance protected interface are classed as protected gateways. Gateways are detected automatically and each is configured with the default maximum bandwidth allowed until configured otherwise.

Table 10: Gateway types

GATEWAY TYPE	DESCRIPTION
protected	All gateways detected or specified connected to the protected interface.
internet	All gateways detected or specified connected to the Internet interface.

The following tables describe the gateway parameters and their formats.

Copyright © 2013, Juniper Networks, Inc

Table 11: Gateway parameters

PARAMETER	VALUE	DESCRIPTION
tospeed	SPEED	The maximum speed that data can be sent to the gateway. If the data trying to be sent to the gateway exceeds this speed then bandwidth defense will be applied.
topkts	PKTS	The maximum packet rate that can be sent to the gateway. If the packet rate to the gateway exceeds this setting then packet rate defense will be applied.

show gateway

Synopsis: `show gateway <internet|protected> <MAC|all|autodetected>`
`show gateway <all>`

Displays the selected gateway configuration.

The second parameter is used to refine the selection of the gateways still further. The value `all` is used to show all defined gateways and their configuration. A value of `<MAC>` displays the gateway with the specified MAC address along with its configuration. The value `autodetected` displays only the MAC address of any auto-detected gateways. Auto-detected gateways are not part of the actual configuration and thus only MAC addresses are listed.

Example:

```
JS>show gateway all
set gateway internet 00:90:27:EA:BF:96 tospeed 0 topkts 10K
set gateway protected 01:02:03:04:05:06 tospeed 100M topkts 37.2K
```

remove gateway

Synopsis: `remove gateway <internet|protected> <MAC|all|autodetected>`

Removes the defined gateway from the configuration.

NOTE: When the value `all`, or `autodetected` is used with the remove gateway command the user is prompted if they are sure. This prompting can be turned off, which may be of use for scripted configurations, see `set terminal confirmations`.

When `autodetected` is used, the command is applied immediately without having to use the `now` parameter or issue the `apply` command.

Example:

```
JS>remove gateway internet all
Are you sure [yes/no]? yes
```

set gateway

Synopsis: `set gateway <internet|protected> <MAC> [tospeed <SPEED>] \`
`[topkts <PKTS>]`

The `set gateway` command can be used to add a new gateway to the configuration, or to change the settings of a gateway already defined in the configuration. The two parameters used determine when bandwidth defense and packet rate defense should be activated. By default, the packet rate defense maximum threshold value `<PKTS>` is 25% of the maximum packet rate of the bandwidth threshold value `<SPEED>` when composed entirely of minimum-size packets (this percentage is increased for speeds less than 8M, and 100%

Copyright © 2013, Juniper Networks, Inc

for speeds less than 2M). A higher value may be needed for a busy gateway heavily used by chat software, but many gateways start to suffer from performance problems when over 50% of their rated bandwidth limit is used to carry small packets alone.

Example:

```
JS>set gateway internet 00:01:02:03:04:05 tospeed 10M
JS>apply
JS>show gateway internet 00:01:02:03:04:05
set gateway internet 00:01:02:03:04:05 tospeed 10M topkts 3720
```

Appliance Mode Configuration

This section describes the global appliance operating settings. The following tables describe the appliance mode parameters and their formats.

Table 12: Appliance Mode Parameters

PARAMETER	VALUE	DESCRIPTION
Hostname	SERVERname	Alternative hostname for the DDoS secure appliance, instead of just the management IP address.
mode	MODE	Current defense mode. See the *Junos DDoS Secure GUI User Guide* for a full description of operational modes.
hamode	HAMODE	Current high availability mode. See the *Junos DDoS Secure GUI User Guide* for a full description of high availability modes.
autoblockenable	yes|no	If enabled, DDoS secure appliance automatically blocks all traffic from the worst offending IP addresses exceeding the autoblockrate thresholds.
autoblockratet1	RATE	The minimum required packet drop rate (type 1) before an IP address is added to the blocked list when automatic blocking is enabled. Whenever a packet is dropped, it is classed as a type 1 drop, or a type 2 drop. Typically, RFC violations are of type 1, and charm decisions / resource consumptions are of type 2. Type 1 rates are usually several orders of magnitude greater than those of type 2.
autoblockratet2	RATE	The minimum required packet drop rate (type 2) before an IP address is added to the blocked list when automatic blocking is enabled.
autoblocksynrst	VALUE	Block IP address if the count exceeds value.
autoblockfragrate	RATE	If fragment re-assemble times out at a rate greater than this, then no fragments are allowed though to the protected IP in question for at least 5 minutes.
autoblockgetrate	rate	If a particular tracked IP keeps accessing a tracked url and the rate is greater that the defined value, the IP address will get automatically blocked.
autonoblock	IPRANGE|none	Never block these IP addresses.

Copyright © 2013, Juniper Networks, Inc

serverautodetect	yes|no	If enabled, protected IPs not previously defined will be protected. If trackindeterminate is enabled, then all IP addresses defined by the DDoS secure appliance Portal are allowed to be automatically included. . If trackindeterminate is not enabled, then all IP addresses defined in the non DDoS secure appliance Portals are allowed to be automatically included.
trackindeterminate	yes|no	Used to determine which set of IP addresses can be auto-detected (see serverautodetect).
testenvironment	yes|no	If set, reduces the time that a connection remains in the closed state to 5 seconds from 60 seconds. This is in violation of the RFCs, but may be needed in a testing environment.
priority	PRIORITY	Active-Standby priority weighting
asymrouting	yes|no	If enabled, session state checking is partially relaxed to mitigate potential timing windows when configured in an asymmetric routing environment. This weakens the protection of internal devices.
groupingid	GROUPINGID	DDoS secure appliances sharing the same grouping id will replicate state information if configured as active-standby.

show appliance

Synopsis: `show appliance`

Displays the current appliance operating settings.

Example:

```
JS>show appliance
set appliance hostname 192.168.0.182 mode defending hamode standalone \
   autoblockenable yes autoblockratet1 200 autoblockratet2 20 autoblocksynrst 300 \
   autoblockfragrate 10 autoblockgetrate 300 autonoblock none serverautodetect yes \
   trackindeterminate yes testenvironment no asymrouting no priority 0 groupingid 15
```

set appliance

Synopsis: `set appliance [hostname <SERVERNAME>] [mode <MODE>] \`
`[hamode <HAMODE>] [autoblockenable <yes|no>] \`
`[autoblockratet1 <RATE>] [autoblockratet2 <RATE>] \`
`[autoblocksynrst <yes|no>] [autoblockfragrate <RATE>] \`
`[autoblockgetrate <yes|no>] [autonoblock <IPRANGE|none>\`
`[serverautodetect <yes|no>] [trackindeterminate <yes|no>] \`
`[testenvironment <yes|no>] [priority <PRIORITY>] \`
`[asymrouting <yes|no>] [groupingid <GROUPINGID>]`

The set appliance command is used to set the global appliance operating settings.

Example:

```
JS>set appliance priority 1
JS>apply
JS>show appliance
set appliance hostname 192.168.0.182 mode defending hamode standalone \
   autoblockenable yes autoblockratet1 200 autoblockratet2 20 autoblocksynrst 300 \
```


Copyright © 2013, Juniper Networks, Inc

```
autoblockfragrate 10 autoblockgetrate 300 autonoblock none serverautodetect yes \
trackindeterminate yes testenvironment no asymrouting no priority 1 groupingid 15
```

Shares Configuration

This section describes the configuration setting for sharing information between DDoS secure appliance Appliances, other than those working in an Active / Standby relationship. The following tables describe the share parameters and their formats.

Table 13: Share Parameters

PARAMETER	VALUE	DESCRIPTION
gateway	IPADDRESS|none	IP address of router gateway to get to destination IP address.
config	yes|no	If enabled, DDoS secure appliance will transmit configuration changes to the specified IP address, to keep configurations in step.
incident	yes|no	If enabled, DDoS secure appliance will transmit incident information to the specified IP address.
state	yes|no	If enabled, DDoS secure appliance will transmit connection state information to the specified address.
required	yes|no	If enabled, if the remote DDoS secure appliance is not available (which could be in a by-pass state), the local DDoS secure appliance will not be so rigorous in state checking.

show share

Synopsis: `show share <IPADDRESS|all>`

Displays the specified share configuration.

Example:

```
JS>show share all
set share 10.1.1.192 gateway none config yes incident yes state yes required no
set share 10.1.1.191 gateway none config yes incident yes state no required no
```

remove share

Synopsis: `remove server <IPADDRESS|all>`

Deletes the specified share. The <*IPADDRESS*> field should have a value that matches an existing defined share IP address. If the IP address used does not match any of the existing defined shares, the command is ignored.

It is also possible to delete all the defined shares. The command `remove share all` deletes all configured shares but prompts for confirmation before the command is accepted.

NOTE: When the value `all` is used with the remove share command the user is prompted if they are sure. This prompting can be turned off, which

Copyright © 2013, Juniper Networks, Inc

may be of use for scripted configurations, see `set terminal confirmations`.

Example:

```
JS>remove share all
Are you sure [yes/no]? yes
```

Example:

```
JS>show share all
set share 10.1.1.192 gateway none config yes incident yes state yes required no
set share 10.1.1.191 gateway none config yes incident yes state no required no
JS>remove share 10.1.1.191
JS>apply
JS>show share all
set share 10.1.1.192 gateway none config yes incident yes state yes required no
```

set share

Synopsis: `set share <IPADDRESS> [gateway <IPADDRESS|none>] \ [config <yes|no>] [incident <yes|no>] [state <yes|no] \ [required <yes|no>]`

If not all parameters are present when defining a new share then any unspecified parameters are automatically set to `no`.

Example:

```
JS>show share all
set share 10.1.1.192 gateway none config yes incident yes state yes required no
JS>set share 10.1.1.191 config yes
JS>apply
JS>show share all
set share 10.1.1.192 gateway none config yes incident yes state yes required no
set share 10.1.1.191 gateway none config yes incident no state no required no
```

Portal Operational Mode Configuration

This section describes the operational mode of a portal.

The following tables describe the operational mode parameters and their formats.

Table 14: Operational Mode Parameters

PARAMETER	VALUE	DEFAULT VALUE	DESCRIPTION
mode	MODEPORTAL	defending	Current defense mode of the Portal. This can be defending or logging.
countries	COUNTRIES|all	all	Defines the countries that are to be permitted by DDoS secure appliance for this Portal. Note: The countries test always is applied to the internet client addresses, not the protected IP addresses.

Copyright © 2013, Juniper Networks, Inc

aslist	ASLIST|all	all	Defines the AS numbers that are to be permitted by DDoS secure appliance for this Portal. Note: The AS numbers test always is applied to the internet client addresses, not the protected IP addresses.

show operation

Synopsis: `show operation`

Displays the current operational mode of the Portal.

Example:

```
JS>show operation
set operation mode defending countries all aslist all
```

set operation

Synopsis: `set operation mode <MODEPORTAL> countries <COUNTRIES> \`

`aslist <ASLIST>`

The set operation command is used to set the operational mode of the Portal.

Example:

```
JS>set operation mode logging
JS>apply
JS>show operation
set operation mode logging countries all aslist all
```

Bandwidth and Port Filter Configuration

DDoS secure appliance has support for user-defined static packet filter rules. A list of filters is associated with a protected IP and the first filter to be matched in the list is used. If there is no filter match, the traffic is dropped. Each filter consists of a name and a set of options. A filter options are used to define what traffic it allows as well as control the bandwidth used.

Once a filter has been defined it can be referenced in later parts of the system configuration for use.

DDoS secure appliance filters themselves are directionless, that is they are not specific to a particular direction of traffic. A filter direction is defined when the filter is named in a filter reference, which has a directional context. Additionally, each filter is stateful. Any traffic a filter allows through in one direction will be associated with a session, that permits corresponding replies back through in the opposite direction. This is an automatic process, so no filter needs to be defined for the corresponding replies.

NOTE: Once a filter is associated with a connection, the bandwidth controls associated with that filter are applied in both directions.

If multiple servers refer to the same filter, then the bandwidth controls are applied as a sum of all the server traffic matching that filter.

Once a TCP filter session is established, the corresponding traffic is allowed to pass until the session completes, even if the original permitting filter is altered or replaced with a stricter filter that would otherwise block (of course, any new traffic sessions will be blocked

Copyright © 2013, Juniper Networks, Inc

if appropriate). However, UDP, ICMP, and other IP filter sessions will be blocked as soon as a new filter is applied that would no longer permit that sessions traffic. An FTP (port 21) filter will also handle the data connections (PORT and PASV) automatically, so no additional filter needs to be defined for ftp.

DDoS secure appliance filtering system has a logical filter named `default`. This is reserved for use as a default filter where no filter selection has been configured. The filter `default` allows all traffic to pass, with the exception of udp port 80, and some ICMP types with no bandwidth restrictions.

There are three other pre-defined filters with names `broadcast`, `multicast` and `redirect`. These filters are applied by default to IP broadcast, multicast and redirect traffic respectively. In contrast to filter `default`, the settings for these pre-defined filters can be altered.

A filter must already be defined before it can be named within an option that expects a filter. A filter can be named against more than one server configuration or filter aggregation.

The following tables describe the filter parameters and their formats.

Table 15: Filter Parameters

PARAMETER	VALUE	DEFAULT VALUE	DESCRIPTION
tcp	PORTLIST	none	The list of ports permitted for TCP connections.
udp	PORTLIST	none	The list of ports permitted for UDP connections.
icmp	ICMPTYPELIST	none	The list of ICMP types permitted.
icmp6	icmptypelist	none	The list of ICMPv6 types permitted.
otherip	PROTOCOLLIST	none	The list of other IP protocols (not TCP, UDP, ICMP or ICMPv6) permitted.
countries	COUNTRIES|all|none	all	Defines the countries that are to be permitted by DDoS secure appliance for this filter. Note: The countries test always is applied to the internet client addresses, not the protected ip addresses.
aslist	ASLIST|all	all	Defines the AS numbers that are to be permitted by DDoS secure appliance for this Portal. Note: The AS numbers test always is applied to the internet client addresses, not the protected IP addresses.
networks	IPRANGE|all|none	all	Defines all the networks (up to 4 entries) that are to be permitted by DDoS secure appliance for this filter. Can be IPv6. Note: The networks test always is applied to the internet client addresses, not the protected ip addresses.
validpkts	PKTS|U	U	Guaranteed packet rate.

Copyright © 2013, Juniper Networks, Inc

burstpkts	PKTS|U	U	Burstable packet rate.
validspeed	SPEED|U	U	Guaranteed bandwidth.
burstspeed	SPEED|U	U	Burstable bandwidth.

show filter

Synopsis: `show filter <FILTERNAME|all>`

Displays the settings of the named filter.

Example:

```
JS>show filter test1
set filter test1 tcp 80 udp none icmp none icmp6 none otherip none countries all \
    networks all aslist all validpkts U burstpkts U validspeed U burstspeed U
```

Alternatively the reserved filter name `all` can be specified to show all defined filters.

Example:

```
JS>show filter all
set filter multicast tcp all udp all icmp 0-18 icmp6 1-4,128-154 otherip all countries all \
   networks all aslist all validpkts U burstpkts U validspeed U burstspeed U
set filter broadcast tcp none udp 1-6,8-65535 icmp none icmp6 none otherip all \
   countries all networks aslist all all validpkts U burstpkts U validspeed U burstspeed U
set filter test1 tcp 80 udp none icmp none icmp6 none otherip none countries all \
   networks all aslist all validpkts U burstpkts U validspeed U burstspeed U
```

NOTE: The logical filter `default` is not listed. Attempts to use `default`, or any non-existent filter name as a parameter to the `show filter` command, results in the error message Not configured. This error is also displayed when the parameter `all` is used but no filters are defined.

remove filter

Synopsis: `remove filter <FILTERNAME|all>`

The remove filter command can be used to delete a specified filter. The specified filter will not be deleted if it is currently assigned to a server. The logical filter default cannot be deleted.

Example:

```
JS>show filter test1
set filter test1 tcp 80 udp none icmp none icmp6 none otherip none countries all \
   networks all aslist all validpkts U burstpkts U validspeed U burstspeed U
JS>remove filter test1
JS>apply
JS>show filter test1
Not configured
```

The `remove filter` command can also be used to delete all filters, as long as none are assigned to a server, by using the reserved filter name `all`. If all the filters cannot be removed then an error message is returned and none are removed. If all the filters can be safely removed, the user will be prompted for confirmation.

Example:

Copyright © 2013, Juniper Networks, Inc

```
JS>show filter all
set filter test1 tcp 80 udp none icmp none icmp6 none otherip none validpkts U \
   countries all networks all aslist all burstpkts U validspeed U burstspeed U
set filter test2 tcp 80,443 udp none icmp none icmp6 none otherip none \
   countries all networks all aslist all validpkts U burstpkts U validspeed U burstspeed U
JS>remove filter all
Are you sure [yes/no]? yes
JS>apply
JS>show filter all
Not configured
```

NOTE: It is possible to turn off prompting which can be useful when using automated scripts (see `set terminal confirmations`).

set filter

Synopsis: `set filter <FILTERNAME> [tcp <PORTLIST|all|none>] \`
`[udp <PORTLIST|all|none>] \`
`[icmp <ICMPTYPELIST|all|none>] \`
`[icmp6 <ICMPTYPELIST|all|none>] \`
`[otherip <PROTOCOLLIST|all|none>] \`
`[countries <COUNTRIES|all|none>] \`
`[networks <IPRANGE|all|none>] \`
`[aslist <ASLIST|all>] \`
`[validpkts <PKTS>] [burstpkts <PKTS>]`
`[validspeed <SPEED>] [burstspeed <SPEED>]`

The `set filter` command is used to create a new filter entry or to modify an existing one. At least a name and one parameter value pair must be specified when using the command. If the name specified does not match an existing filter entry, a new entry is created with that name and any parameter value pair not specified causes that parameter to be set with the default value. If an entry already exists that matches the name specified then only the parameter value pairs specified are altered.

The following protocol numbers have no effect when used as values with the otherip parameter, as these protocols are handled separately by their own parameter value pair:

- 1 (ICMP)
- 6 (TCP)
- 17 (UDP)
- 58 (ICMPv6)

Example:

```
JS>show filter all
set filter test1 tcp 80 udp none icmp none icmp6 none otherip none countries \
   all networks all aslist all validpkts U burstpkts U validspeed U burstspeed U
set filter test2 tcp 80,443 udp all icmp none icmp6 none otherip none countries all \
   networks all aslist all validpkts U burstpkts U validspeed U burstspeed U
JS>set filter test1 tcp 80-85,443
JS>set filter test2 udp none icmp 8
JS>apply
JS>show filter all
set filter test1 tcp 80-85,443 udp none icmp none icmp6 none otherip none countries \
   all networks all aslist all validpkts U burstpkts U validspeed U burstspeed U
```


Copyright © 2013, Juniper Networks, Inc

```
set filter test2 tcp 80,443 udp none icmp 8 otherip none icmp6 none countries all \
   networks all aslist all validpkts U burstpkts U validspeed U burstspeed U
```

Filter Aggregation Configuration

Servers require a list of one or more filters when determining what traffic to allow. This list is searched for the first match and then used. To aid configuring these lists, filter aggregations are used to define a list of up to seven filters. A filter aggregation may refer to a (previously defined) filter aggregation to extend the list.

A filter aggregation must already be defined before it can be named within an option that expects a filter or filter aggregation. A filter aggregation can be named against more than one server configuration or filter aggregation.

The following tables describe the filter aggregation parameters and their formats.

Table 16: Filter Aggregation Parameters

PARAMETER	VALUE	DEFAULT VALUE	DESCRIPTION
filtera	FILTERNAME	-undefined-	The name of the filter or filter aggregation to check against.
filterb	FILTERNAME	-undefined-	The name of the filter or filter aggregation to check against.
filterc	FILTERNAME	-undefined-	The name of the filter or filter aggregation to check against.
filterd	FILTERNAME	-undefined-	The name of the filter or filter aggregation to check against.
filtere	FILTERNAME	-undefined-	The name of the filter or filter aggregation to check against.
filterf	FILTERNAME	-undefined-	The name of the filter or filter aggregation to check against.
filterg	FILTERNAME	-undefined-	The name of the filter or filter aggregation to check against.

Table 17: Filter Fixed Value Formats

PARAMETER VALUE	DESCRIPTION
-undefined-	Entry not in use

show fagg

Synopsis: `show fagg <`*`FILTERNAME`*`|all>`

Displays the settings of the named filter aggregation.

Example:

```
JS>show fagg web-agg
set fagg web-agg filtera web filterb default filterc –undefined- filterd –undefined- \
    filtere –undefined- filterf –undefined- filterg –undefined-
```

Alternatively the reserved filter name `all` can be specified to show all defined filters.

Example:

```
JS>show fagg all
```

Copyright © 2013, Juniper Networks, Inc

```
set fagg web-agg filtera web filterb default filterc -undefined- filterd -undefined- \
    filtere -undefined- filterf -undefined- filterg -undefined-
set fagg example-agg filtera default filterb -undefined- filterc -undefined- \
    filterd -undefined- filtere -undefined- filterf -undefined- filterg -undefined-
```

remove fagg

Synopsis: `remove fagg <FILTERNAME|all>`

The remove fagg command can be used to delete a specified filter aggregation. The specified filter aggregation will not be deleted if it is currently assigned to a server.

Example:

```
JS>show fagg web-agg
set fagg web-agg filtera web filterb default filterc -undefined- filterd -undefined- \
    filtere -undefined- filterf -undefined- filterg -undefined-
JS>remove fagg web-agg
JS>apply
JS>show fagg web-agg
Not configured
```

The `remove fagg` command can also be used to delete all filter aggregations, as long as none are assigned to a server, by using the reserved filter name `all`. If all the filter aggregations s cannot be removed then an error message is returned and none are removed. If all the filter aggregations can be safely removed, the user will be prompted for confirmation.

Example:

```
JS>show fagg all
set fagg web-agg filtera web filterb default filterc -undefined- filterd -undefined- \
    filtere -undefined- filterf -undefined- filterg -undefined-
set fagg example-agg filtera default filterb -undefined- filterc -undefined- \
    filterd -undefined- filtere -undefined- filterf -undefined- filterg -undefined-
JS>remove fagg all
Are you sure [yes/no]? yes
JS>apply
JS>show fagg all
Not configured
```

NOTE: It is possible to turn off prompting which can be useful when using automated scripts (see `set terminal confirmations`).

set fagg

Synopsis: `set fagg <FILTERNAME> [filtera <FILTERNAME|-undefined->] \`
`[filterb <FILTERNAME|-undefined->] \`
`[filterc <FILTERNAME|-undefined->] \`
`[filterd <FILTERNAME|-undefined->] \`
`[filtere <FILTERNAME|-undefined->] \`
`[filterf <FILTERNAME|-undefined->] \`
`[filterg <FILTERNAME|-undefined->]`

The `set fagg` command is used to create a new filter aggregation entry or to modify an existing one. At least a name and one parameter value pair must be specified when using the command. If the name specified does not match an existing filter entry, a new entry is created with that name and any parameter value pair not specified causes that parameter to be set with the default value. If an entry already exists that matches the name specified then only the parameter value pairs specified are altered.

Copyright © 2013, Juniper Networks, Inc

Example:

```
JS>show fagg all
set fagg web-agg filtera web filterb default filterc -undefined- filterd -undefined- \
    filtere -undefined- filterf -undefined- filterg -undefined-
set fagg example-agg filtera default filterb -undefined- filterc -undefined- \
    filterd -undefined- filtere -undefined- filterf -undefined- filterg -undefined-
JS>set fagg web-agg filterg webplus
JS>apply
JS>show fagg all
set fagg web-agg filtera web filterb default filterc -undefined- filterd -undefined- \
    filtere -undefined- filterf -undefined- filterg webplus
set fagg example-agg filtera default filterb -undefined- filterc -undefined- \
    filterd -undefined- filtere -undefined- filterf -undefined- filterg -undefined-
```

Protected IP Configuration

The following tables describe the protected IP parameters and their formats.

Table 18: Protected IP Parameters

PARAMETER	VALUE	DESCRIPTION
name	PROTECTEDNAME	The text name of the protected IP. This parameter is ignored when defining settings for the default protected IP.
backlog	BACKLOG	The TCP backlog setting. Refer to the *Junos DDoS Secure GUI User Guide* for further details.
connections	CONNECTIONS	The maximum number of connections. Refer to the *Junos DDoS Secure GUI User Guide* for further details.
connrate	CONNRATE	The maximum connection rate. Refer to the *Junos DDoS Secure GUI User Guide* for further details.
gets	GETS	The maximum concurrent number of active GET / HEAD / POST that a protected IP can handle at once. An example is IISs ASP thread count.
infilter	FILTERNAME	The filter used for inbound connections.
outfilter	FILTERNAME	The filter used for outbound connections.
sendtcprejects	yes|no	Send tcp rejects for a tcp connection that does not match any filters.
soap	yes|no	Look for Soap Action headers to differentiate URLs.
fragsdisabled	yes|no	Specifies whether fragments are allowed for this protected IP.
mode	MODEIP	Specifies the mode that het protected IP is running under.

show protected

Synopsis: `show protected <IPADDRESS|all|default|indeterminate| \ broadcast|multicast|redirect|autodetected>`

Copyright © 2013, Juniper Networks, Inc

Displays the specified protected IP configuration.

Example:

```
JS>show protected all
set protected default backlog auto-1000 connections auto-1000 connrate auto-1000 \
   gets auto-1000 infilter inbound outfilter outbound sendtcprejects no soap no \
   fragsdisabled no mode defending
set protected multicast backlog auto-1000 connections auto-1000 connrate auto-1000 \
   gets auto-1000 infilter multicast outfilter multicast sendtcprejects no soap no \
   fragsdisabled no mode defending
set protected broadcast backlog auto-1000 connections auto-1000 connrate auto-1000 \
   gets auto-1000 infilter broadcast outfilter broadcast sendtcprejects no soap no \
   fragsdisabled no mode defending
set protected indeterminate backlog auto-1000 connections auto-1000 \
   connrate auto-1000 gets auto-1000 infilter default outfilter default \
   sendtcprejects no soap no fragsdisabled no mode defending
set protected 10.50.1.1 backlog 1000 connections 5000 connrate 100 gets U \
   infilter default outfilter default sendtcprejects yes soap no fragsdisabled no \
   mode defending
set protected 10.50.2.1 backlog 1000 connections 5000 connrate 100 gets U \
   infilter default outfilter default sendtcprejects yes soap no fragsdisabled no \
   mode defending
```

remove protected

Synopsis: `remove protected <IPADDRESS|all|autodetected>`

Deletes the specified protected IP. The <*IPADDRESS*> field should have a value that matches an existing defined protected IP address, an auto-detected preotected entry is not considered a defined protected IP. If the IP address used does not match any of the existing defined protected IPs, the command is ignored.

It is also possible to delete all the defined protected IPs. The command `remove protected all` deletes all configured protected IPs but prompts for confirmation before the command is accepted. The default protected parameters are not altered by the use of the value `all`. The default, indeterminate, multicast, broadcast and `redirect` protected IP settings cannot be removed.

NOTE: When the value `all`, or `autodetected` is used with the remove protected command the user is prompted if they are sure. This prompting can be turned off, which may be of use for scripted configurations, see `set terminal confirmations`.

When `autodetected` is used, the command is applied immediately without having to use the `now` parameter or issue the `apply` command.

Example:

```
JS>remove protected all
Are you sure [yes/no]? yes
```

Example:

```
JS>show protected all
set protected default backlog auto-1000 connections auto-1000 connrate auto-1000 \
   gets auto-1000 infilter inbound outfilter outbound sendtcprejects no soap no \
   fragsdisabled no mode defending
set protected multicast backlog auto-1000 connections auto-1000 connrate auto-1000 \
   gets auto-1000 infilter multicast outfilter multicast sendtcprejects no soap no \
   fragsdisabled no mode defending
```


Copyright © 2013, Juniper Networks, Inc

```
set protected broadcast backlog auto-1000 connections auto-1000 connrate auto-1000 \
   gets auto-1000 infilter broadcast outfilter broadcast sendtcprejects no soap no \
   fragsdisabled no mode defending
set protected indeterminate backlog auto-1000 connections auto-1000 \
   connrate auto-1000 gets auto-1000 infilter default outfilter default \
   sendtcprejects no soap no fragsdisabled no mode defending
set protected 10.50.1.1 backlog 1000 connections 5000 connrate 100 gets U \
   infilter default outfilter default sendtcprejects yes soap no fragsdisabled no \
   mode defending
set protected 10.50.2.1 backlog 1000 connections 5000 connrate 100 gets U \
   infilter default outfilter default sendtcprejects yes soap no fragsdisabled no \
   mode defending
JS>remove server 10.50.1.1
JS>apply
JS>show protected all
set protected default backlog auto-1000 connections auto-1000 connrate auto-1000 \
   gets auto-1000 infilter inbound outfilter outbound sendtcprejects no soap no \
   fragsdisabled no mode defending
set protected multicast backlog auto-1000 connections auto-1000 connrate auto-1000 \
   gets auto-1000 infilter multicast outfilter multicast sendtcprejects no soap no \
   fragsdisabled no mode defending
set protected broadcast backlog auto-1000 connections auto-1000 connrate auto-1000 \
   gets auto-1000 infilter broadcast outfilter broadcast sendtcprejects no soap no \
   fragsdisabled no mode defending
set protected indeterminate backlog auto-1000 connections auto-1000 \
   connrate auto-1000 gets auto-1000 infilter default outfilter default \
   sendtcprejects no soap no fragsdisabled no mode defending
set protected 10.50.2.1 backlog 1000 connections 5000 connrate 100 gets U \
   infilter default outfilter default sendtcprejects yes soap no fragsdisabled no \
   mode defending
```

set protected

Synopsis: `set protected \`
`<`*`IPADDRESS`*`|default|indeterminate|multicast|broadcast> \`
`[name <`*`PROTECTEDNAME`*`>] [backlog <`*`BACKLOG`*`|auto-`*`BACKLOG`*`>]\`
`[connections <`*`CONNECTIONS`*`|auto-`*`CONNECTIONS`*`>] \`
`[connrate <`*`CONNRATE`*`|auto-`*`CONNRATE`*`>] \`
`[gets <`*`GETS`*`|auto-`*`GETS`*`>] \`
`[infilter <`*`FILTERNAME`*`|default>] \`
`[outfilter <`*`FILTERNAME`*`|default>] \`
`[sendtcprejects <yes|no>] [soap <yes|no>] \`
`[fragsdisabled <yes|no>] [mode <`*`MODEIP`*`>]`

If not all parameters are present when defining a new protected IP then any unspecified parameters are automatically set to those of the default protected IP.

Example:

```
JS>show protected all
set protected default backlog auto-1000 connections auto-1000 connrate auto-1000 \
   gets auto-1000 infilter inbound outfilter outbound sendtcprejects no soap no \
   fragsdisabled no mode defending
set protected multicast backlog auto-1000 connections auto-1000 connrate auto-1000 \
   gets auto-1000 infilter multicast outfilter multicast sendtcprejects no soap no \
   fragsdisabled no mode defending
set protected broadcast backlog auto-1000 connections auto-1000 connrate auto-1000 \
   gets auto-1000 infilter broadcast outfilter broadcast sendtcprejects no soap no \
   fragsdisabled no mode defending
```

Copyright © 2013, Juniper Networks, Inc

```
set protected indeterminate backlog auto-1000 connections auto-1000 \
   connrate auto-1000 gets auto-1000 infilter default outfilter default \
   sendtcprejects no soap no fragsdisabled no mode defending
set protected 10.50.2.1 backlog 1000 connections 5000 connrate 100 gets U \
   infilter default outfilter default sendtcprejects yes soap no fragsdisabled no \
   mode defending
JS>set server 10.50.1.1 infilter default outfilter default
JS>apply
JS>show protected all
set protected default backlog auto-1000 connections auto-1000 connrate auto-1000 \
   gets auto-1000 infilter inbound outfilter outbound sendtcprejects no soap no \
   fragsdisabled no mode defending
set protected multicast backlog auto-1000 connections auto-1000 connrate auto-1000 \
   gets auto-1000 infilter multicast outfilter multicast sendtcprejects no soap no \
   fragsdisabled no mode defending
set protected broadcast backlog auto-1000 connections auto-1000 connrate auto-1000 \
   gets auto-1000 infilter broadcast outfilter broadcast sendtcprejects no soap no \
   fragsdisabled no mode defending
set protected indeterminate backlog auto-1000 connections auto-1000 \
   connrate auto-1000 gets auto-1000 infilter default outfilter default \
   sendtcprejects no soap no fragsdisabled no mode defending
set protected 10.50.1.1 backlog auto-1000 connections auto-1000 connrate auto-1000 \
   gets U infilter default outfilter default sendtcprejects yes soap no \
   fragsdisabled no mode defending
set protected 10.50.2.1 backlog 1000 connections 5000 connrate 100 gets U \
   infilter default outfilter default sendtcprejects yes soap no fragsdisabled no \
   mode defending
```

Portal Defense Configuration

The following tables describe the Portal Defense parameters and their formats. An example for a portal could be a load balancer with multiple VIPs. Portal Defense could then be used to protect this load balancer from overload.

Table 19: Portal Defense Parameters

PARAMETER	VALUE	DESCRIPTION
backlog	BACKLOG	The TCP backlog setting. Refer to the *Junos DDoS Secure GUI User Guide* for further details.
connections	CONNECTIONS	The maximum number of connections. Refer to the *Junos DDoS Secure GUI User Guide* for further details.
connrate	CONNRATE	The maximum connection rate. Refer to the *Junos DDoS Secure GUI User Guide* for further details.
gets	GETS	The maximum concurrent number of active GET / HEAD / POST that a server can handle at once. An example is IIS ASP thread count.

show portaldefense

Synopsis: `show portaldefense`

Displays the portal defense configuration.

Example:

Copyright © 2013, Juniper Networks, Inc

```
JS>show portal defense
set portaldefense backlog U connections U connrate U gets U
```

set portaldefense

Synopsis: `set portaldefense \`
`[backlog <BACKLOG|auto-BACKLOG>] \`
`[connections <CONNECTIONS|auto-CONNECTIONS>] \`
`[connrate <CONNRATE|auto-CONNRATE>] \`
`[gets <GETS|auto-GETS>]`

If not all parameters are present when defining the portal defense then any unspecified parameters are automatically set to those of the default server.

Example:

```
JS>set portaldefense backlog 10000 connections U connrate U gets U
JS>apply
JS>show portaldefense
set portaldefense backlog 10000 connections U connrate U gets U
```

Block Country and IPs Configuration

The following tables describe the block parameters and their formats.

Table 20: Block Parameters

PARAMETER	VALUE	DESCRIPTION
country	COUNTRIES|all|none	Defines the countries that are to be blocked by DDoS secure appliance.
IP	IPRANGE|none	Defines the list of IP address and networks that are to be blocked by DDoS secure appliance.

show block

Synopsis: `show block`

Displays the current blocked countries and IP addresses.

Example:

```
JS>show block
set block country none
set block cignoreip none
set block ip none
set block as none
```

set block country

Synopsis: `set block country <COUNTRIES|none>`

It is possible that there may be an attack originating in a specific country and you want to drop all traffic to or from that country for the duration of the attack. It is possible to specify a list of countries, and IP addresses tagged by MaxMind as being in these countries will get blocked. This requires that the MaxMind database is periodically updated.

Example:

```
JS>set block country USA
JS>apply
```

Copyright © 2013, Juniper Networks, Inc

```
JS>show block
set block country USA
set block cignoreip none
set block ip none
set block as none
```

set block cignoreip

Synopsis: `set block cignoreip <IPRANGE|none>`

It is possible that there may be an attack originating in a specific country and you want to drop all traffic to or from that country for the duration of the attack. However, you may want to allow specific trusted IPs from that country access.

Example:

```
JS>set block cignoreip 1.2.3.4
JS>apply
JS>show block
set block country USA
set block cignoreip 1.2.3.4
set block ip none
set block as none
```

set block ip

Synopsis: `set block ip <IPRANGE|none>`

It is possible that there may be an attack originating from a specific set of addresses and you want to permanently drop all traffic to or from those IP addresses. It is possible to specify a list of ips or networks, comma separated.

Example:

```
JS>set block ip 10.20.0.0/25
JS>apply
JS>show block
set block country USA
set block cignoreip none
set block ip 10.20.0.0/25
set block as none
```

set block as

Synopsis: `set block as <ASLIST|none>`

It is possible that there may be an attack originating from a specific AS and you want to permanently drop all traffic to or from that AS. It is possible to specify a list of AS numbers, comma separated.

Example:

```
JS>set block as 65001
JS>apply
JS>show block
set block country USA
set block cignoreip none
set block ip 10.20.0.0/25
set block as 65001
```

Country Code (geoip) Definitions

Copyright © 2013, Juniper Networks, Inc

It is possible specify Country Codes for specific IP addresses that override the MaxMind definitions or to categorize pseudo countries for ease of control of blocks of addresses. This is done by:

Define the Country Code with a list of IP addresses.

Specify a url to download the list of IP addresses from. These IP addresses are held in a flat file, line delimited, each line being an IP address, a Subnet or IP range of addresses.

Several Country Codes have a special significance.

-bl	Any IP Addresses matching this code will always get black-listed.
-wl	Any IP Addresses matching this code will always get white-listed.
-pl	Any IP Addresses matching this code will be treated as a Preferred Client.
-wn	Any IP Addresses matching this code will always get white-listed, but no logs generated.

The IP lookup database is built in the following order, with subsequent entries overwriting any previous IP definitions.

- Maxmind Information
- Bogon list (which contains RFC1918 addresses defined as bogons) http://www.cymru.com/Documents/bogon-bn-agg.txt.
- RFC 1918 Addresses
- User Definitions specified by geoip entries

Table 21: Geoip Parameters

PARAMETER	VALUE	DESCRIPTION
code	COUNTRYCODE	Defines the country code that is to be set.
IP	IPRANGE	Defines the list of IP address and networks that are to be associated with the country code.
frequency	FREQUENCY	Frequency at which the URL is checked for updates.
url	URL	The URL containing the list of IP addresses, line separated, IPRANGE per line.
Header	HEADER	Matches Header definition, including trailing :

show geoip

Synopsis: `show geoip \`
`<all|ip|url|megaproxy_ip|megaproxy_url|auto_akamai>`

Displays the current geoip definition list.

Example:

```
JS>show geoip all
No geoip definitions set up
```

remove geoip

Synopsis: `remove geoip \`
`<all|ip|url|megaproxy_ip|megaproxy_url|auto_akamai >`

Copyright © 2013, Juniper Networks, Inc

Deletes the current inspection list

Example:

```
JS>remove geoip all
JS>apply
JS>show geoip all
No geoip definitions set up
```

set geoip ip

Synopsis: `set geoip ip code <COUNTRYCODE> ip <IPRANGE>`

set geoip url

Synopsis: `set geoip url code <COUNTRYCODE> freq <FREQUENCY> \
url <URL>`

set geoip megaproxy_ip

Synopsis:
```
set geoip megaproxy_ip header <HEADER> \
          respcode <RESPCODE> ip <IPLIST>
```

set geoip megaproxy_url

Synopsis:
```
set geoip megaproxy_url header <HEADER> \
          respcode <RESPCODE> freq <FREQUENCY> url <URL>
```

set geoip auto_akamai

Synopsis: `set geoip auto_akamai respcode <RESPCODE>`

This allows for the updating of IP addresses with Country Codes by different methods.

The auto_akamai is looking for proxy servers that include the True-Client-IP: header.

Example:

```
JS>set geoip url code –bl freq h http://black.list.com/list.txt
JS>set geoip megaproxy_ip header X-Forwarded-For: respcode 503 ip 1.2.3.4
JS>apply
JS>show geoip all
set geoip url code –bl freq h http://black.list.com/list.txt
set geoip megaproxy_ip header X-Forwarded-For: respcode 503 ip 1.2.3.4
```

Preferred Clients and White-Listing Configuration

The following tables describe the preferred parameters and their formats.

Table 22: Preferred Parameters

PARAMETER	VALUE	DESCRIPTION
clients	IPRANGE|none	Defines the client IP addresses (on the Internet side of the DDoS secure appliance) get preferential treatment by giving them a CHARM boost.
countries	COUNTRIES|none	Defines which Countries get preferential treatment by giving them a CHARM boost.
default	IPRANGE|none	Defines the client IP addresses (on the Internet side of the DDoS secure appliance) always get the default CHARM scoring.

Copyright © 2013, Juniper Networks, Inc

whitelisted	IPRANGE|none	Defines the client network (on the Internet side of the DDoS secure appliance) that can be used for pen-testing. All packets coming from a white-listed network are passed through as if the DDoS secure appliance was operating in Logging.There is therefore no protection for the protected IPs by DDoS secure appliance for any packets coming from this network address.
whitenolog	IPRANGE|none	Defines the client network (on the Internet side of the DDoS secure appliance) that can be used for pen-testing. All packets coming from a white-list network are passed through as if the DDoS secure appliance was operating in Logging. There is therefore no protection for the protected IPs by DDoS secure appliance for any packets coming from this network address. Note: None of this traffic is logged

show preferred

Synopsis: `show preferred \ [all|clients|countries|whitenolog|whitelisted|default]`

Displays the current clients and pen-test networks.

Example:

```
JS>show preferred all
set preferred clients none
set preferred whitenolog 192.168.213.0/24,172.16.166.0/24
set preferred whitelisted none
set preferred default none
set preferred countries none
```

set preferred clients

Synopsis: `set preferred clients <IPLIST|none>`

It is possible that there may be some client addresses that need preferential treatment by the DDoS secure appliance Charm engine when the protected servers are under load / attack conditions. By specifying these IP addresses in the preferred clients list, these IP addresses will get a charm boost when charm is calculated. If these IP addresses misbehave badly, packets from these IP addresses may still get dropped.

Example:

```
JS>set preferred clients 192.168.10.1
JS>apply
JS>show preferred clients
set preferred clients 192.168.10.1
```

set preferred countries

Synopsis: `set preferred countries <COUNTRIES|none>`

It is possible that there may be some countries that need preferential treatment by the DDoS secure appliance Charm engine when the protected servers are under load / attack conditions. By specifying these Countries in the preferred countries list, the IP addresses from these Countries will get a charm boost when charm is calculated. If the IP addresses from these Countries misbehave badly, packets from these IP addresses may still get dropped.

Example:

```
JS>set preferred countries GBR
JS>apply
```

Copyright © 2013, Juniper Networks, Inc

```
JS>show preferred countries
set preferred countries GBR
```

set preferred whitelist

Synopsis: `set preferred whitelist <IPRANGE|none>`

If there is a client network that needs to pen-test servers through the DDoS secure appliance, even if the IP addresses are specified as `preferred clients`, it is likely that the pen-test traffic will get blocked. The `preferred whitelist` option effectively makes the DDoS secure appliance engine run in Logging mode for the defined whitelisted network addresses. For all other IP addresses, the DDoS secure appliance engine will run in the defined Appliance mode.

Example:

```
JS>set preferred whitelisted 10.20.0.0/25
JS>apply
JS>show preferred whitelisted
set preferred whitelisted 10.20.0.0/25
```

set preferred whitenolog

Synopsis: `set preferred whitenolog <IPRANGE|none>`

If there is a client network that needs to pen-test servers through the DDoS secure appliance, even if the IP addresses are specified as `preferred clients`, it is likely that the pen-test traffic will get blocked. The `preferred whitenolog` option effectively makes the DDoS secure appliance engine run in Logging mode for the defined whitelisted network addresses. For all other IP addresses, the DDoS secure appliance engine will run in the defined Appliance mode.

NOTE: Any misbehaving activity to/from these IP addresses will not get logged anywhere.

Example:

```
JS>set preferred whitenolog 10.30.0.0/25
JS>apply
JS>show preferred whitenolog
set preferred whitelisted 10.30.0.0/25
```

set preferred default

Synopsis: `set preferred default <IPLIST|none>`

It is possible that there may be some client addresses that always need default treatment by the DDoS secure appliance Charm engine when the protected servers are under load / attack conditions. By specifying these IP addresses in the preferred default list, these IP addresses will always get the default charm when charm is calculated. If these IP addresses misbehave badly, packets from these IP addresses may still get dropped.

NOTE: Examples could be web site availability monitors.

Example:

```
JS>set preferred default 192.168.20.1
JS>apply
JS>show preferred default
```


Copyright © 2013, Juniper Networks, Inc

```
set preferred clients 192.168.20.1
```

Layer 7 Inspection

It is possible to inspect certain Layer 7 requests, and give weightings (negative CHARM bias) to specific requests to discourage repeated access to these requests. This bias is also added to the Worst Offenders Resource Usage average rate, so must have a value that is less than `autoblockratet2` (see `set appliance`). Currently, inspection of the http urls and dns queries is supported. Matching is defined by:-

- The matching of the entire request, including parameters.
- The matching of the initial part of the request, which can possibly include some parameters.
- The use of Basic Regular Expression syntax.
- The use of Extended Regular Expression syntax. To prevent unexpected matches–an example would be / which would match on any / in the URL and it does not mean a request for the home page–it is suggested that the ^ and $ anchors are used.

Where possible, it is recommended that matching methods 1 and 2 be used for performance reasons.

show inspect

Synopsis: `show inspect <all| \`
`url_match <all|`*`STRING`*`>|url_prefix <all|`*`STRING`*`>| \`
`url_regex <all|`*`REGEX`*`>|url_eregex <all|`*`EREGEX`*`> | \`
`dns_match <all|`*`STRING`*`>|dns_prefix <all|`*`STRING`*`>| \`
`dns_regex <all|`*`REGEX`*`>|dns_eregex <all|`*`EREGEX`*`> | \`
`sip_match <all|`*`STRING`*`>|sip_prefix <all|`*`STRING`*`>| \`
`sip_regex <all|`*`REGEX`*`>|sip_eregex <all|`*`EREGEX`*`> | \`
`sip_eregex <all|`*`REGEX`*`>|sip_eregex <all|`*`EREGEX`*`> >`

Displays the current inspection list and weighting.

Example:

```
JS>show inspect all
Inspect disabled
```

remove inspect

Synopsis: `remove inspect <all| \`
`url_match <all|`*`STRING`*`>|url_prefix <all|`*`STRING`*`>| \`
`url_rgex <all|`*`REGEX`*`>|url_eregex <all|`*`EREGEX`*`> | \`
`dns_match <all|`*`STRING`*`>|dns_prefix <all|`*`STRING`*`>| \`
`dns_regex <all|`*`REGEX`*`>|dns_eregex <all|`*`EREGEX`*`> | \`
`sip_match <all|`*`STRING`*`>|sip_prefix <all|`*`STRING`*`>| \`
`sip_regex <all|`*`REGEX`*`>|sip_eregex <all|`*`EREGEX`*`> >`

Deletes the current inspection list.

Example:

```
JS>remove inspect all
JS>apply
JS>show inspect all
Inspect disabled
```

set inspect

Copyright © 2013, Juniper Networks, Inc

Synopsis: `set inspect < \`
`url_match <STRING>|url_prefix <STRING>| \`
`url_regex <REGEX>|url_eregex <EREGEX> | \`
`dns_match <STRING>|dns_prefix <STRING>| \`
`dns_regex <REGEX>|dns_eregex <EREGEX> | \`
`dns_match <STRING>|sip_prefix <STRING>| \`
`dns_regex <REGEX>|sip_eregex <EREGEX> |`
`<bl|-bl|wl|BIAS> >`

This allows for the checking of specific Layer 7 requests by different inspection methods.

Example:

```
JS>set inspect url_regex ^/index.asp$ 10
JS>apply
JS>show inspect all
set inspect url_regex "^/index.asp$" 10
```

Disable RFC testing

It is possible to disable some of the RFC compliancy checking, but this does provide a security risk for the protected servers. Not all the RFC checking is configurable.

Table 23: Disable Parameters

PARAMETER	VALUE	DESCRIPTION
all	yes|no	Disables all the optional RFC checking.
badudppacket_no_data	yes|no	Disables checking for UDP packets with no data.
tcpattack_nodata	yes|no	Disables no data transfer alerting
blockedstate_invalidstate	yes|no	Disables invalid tcp state alerting
blockedstate_nostate	yes|no	Disables no tcp state alerting

show disabled

Synopsis: `show disabled`

Displays the current RFC disabled state.

Example:

```
JS>show disabled
Nothing disabled
```

set disabled

Synopsis: `set disabled <all|badudppacket_nodata|tcpattack_nodata| \`
`blockedstate_invalidstate|blockedstate_nostate> <yes|no>`

This allows specific RFC checks to be disabled.

Example:

```
JS>set disabled all yes
JS>apply
JS>show disabled
set disabled unknownsession_nostate yes unknownsession_invalidstate yes \
badudppacket_nodata yes tcpattack_nodata yes
```


Copyright © 2013, Juniper Networks, Inc

TCP State Timeouts

It is possible to change the TCP State timeouts from their default values. Changing these values to low numbers can have a detrimental affect on the traffic flows and should only be done under the guidance of a DDoS secure appliance engineer.

Table 24: Timeout parameters

PARAMETER	VALUE	DEFAULT VALUE	SENDS KEEP-ALIVE	SENDS RST ON SESSION END *
syn	STATETIMEOUT|default	10 seconds		
s-a	STATETIMEOUT|default	7 seconds		Yes
s-s	STATETIMEOUT|default	10 seconds		
ack	STATETIMEOUT|default	60 seconds		Yes
p-a	STATETIMEOUT|default	60 seconds		Yes
get	STATETIMEOUT|default	15 minutes		Yes
est	STATETIMEOUT|default	15 minutes	Yes	Yes
f1s	STATETIMEOUT|default	3 minutes	Yes	Yes
f2s	STATETIMEOUT|default	3 minutes	Yes	Yes
f3s	STATETIMEOUT|default	70 seconds		
f-f	STATETIMEOUT|default	70 seconds		Yes
f1d	STATETIMEOUT|default	3 minutes	Yes	Yes
f2d	STATETIMEOUT|default	3 minutes	Yes	Yes
f3d	STATETIMEOUT|default	70 seconds		
cls	STATETIMEOUT|default	70 seconds		
rst	STATETIMEOUT|default	30 seconds		
r-c	STATETIMEOUT|default	30 seconds		
unk	STATETIMEOUT|default	70 seconds		
Spf	STATETIMEOUT|default	10 seconds		
Sif	STATETIMEOUT|default	10 seconds		
gets	STATETIMEOUT|default	2 minutes		

Copyright © 2013, Juniper Networks, Inc

ack80	STATETIMEOUT|default	20 seconds	Yes
url	STATETIMEOUT|default	10 seconds	
f2d80	STATETIMEOUT|default	20 seconds	Yes
Swin	STATETIMEOUT|default	2 minutes	

* Only if Source and Destination IPs of the session are both in defending mode.

show timeout

Synopsis: `show timeout [all|default]`

Displays the current state timeouts that do not have the default values, or all the default values.

Example:

```
JS>show timeout all
No timeout changes
```

set timeout

Synopsis: `set timeout <PARAMETER> <VALUE> […]`

The *<PARAMETER> <VALUE>* pair are taken from the Timeout parameters table above.

Example:

```
JS>set timeout s-a 25
JS>apply
JS>show timeout all
set timeout s-a 25
```

CHARM Tuneables

Changing these values should only be done under the guidance of a DDoS secure appliance engineer and any changes will affect the CHARM weighting values.

Table 25: Tuneable Parameters

PARAMETER	VALUE	DESCRIPTION
charmgetratebias	BIAS	10
charmconnratebias	BIAS	1
Charmconnbias	BIAS	1

show tuneable

Synopsis: `show tuneable [all|default]`

Displays the tuneable information.

Example:

```
JS>show tuneable all
set tuneable charmgetratebias 10
```

remove tuneable

Copyright © 2013, Juniper Networks, Inc

Synopsis: `remove tuneable all`

Deletes the current tuneable definitions

Example:

```
JS>remove tuneable all
JS>apply
JS>show tuneable all
tuneable disabled
```

set tuneable

Synopsis: `set tuneable <charmgetratebias|charmconnratebias|charmconnbias> <BIAS>`

This allows specific CHARM biases to be modified..

Example:

```
JS>set tuneable charmgetratebias 10
JS>apply
JS>show tuneable
set tuneable charmgetreatebias 10
```

Date and Time

The following tables describe the date and time parameters and their formats.

Table 26: Date and Time Parameters

PARAMETER	VALUE	DESCRIPTION
timenow	TIMESTRING	The date and time
timezone	TIMEZONE	The time zone for displaying date and time
Ntp	IPLIST	NTP server(s) with which to synchronize

show clock

Synopsis: `show clock`

Displays the current time, timezone and NTP server configured.

Example:

```
JS>show clock
set clock timenow 2003-01-15T15:26:27
set clock timezone Europe/London
set clock ntp none
```

set clock timenow

Synopsis: `set clock timenow <TIMESTRING>`

It is important to set the system timezone to the correct value before adjusting the clock time (see `set clock timezone`). This is because the `set clock timenow` command assumes that all time values entered are offset from UTC time by the local timezone. If the local time is configured while the timezone is set to a region with a different time offset from UTC, the clock will effectively be wrong by the number of hours separating the current local

Copyright © 2013, Juniper Networks, Inc

timezone from the system set timezone. This difference will clear when the system timezone value is corrected.

NOTE: This command is applied immediately without having to use the `now` parameter or issue the `apply` command.

Examples:

```
JS>show clock timenow
set clock timenow 2003-01-24T14:21:27
JS>set clock timenow 2003-01-24T14:00:00
JS>show clock timenow
set clock timenow 2003-01-24T14:00:02

JS>set clock timenow "24 jan 2003 15:00:00"
JS>show clock timenow
set clock timenow 2003-01-24T15:00:03

JS>set clock timenow "24-jan-03 16:00:00"
JS>show clock timenow
set clock timenow 2003-01-24T16:00:03

JS>set clock timenow "jan 24 17:00:00 2003"
JS>show clock timenow
set clock timenow 2003-01-24T17:00:02
```

set clock timezone

Synopsis: `set clock timezone <TIMEZONE>`

Sets the timezone of the appliance. A complete list of valid timezones can be displayed using the `show timezones` command.

Example:

```
JS>show clock
set clock timenow 2003-08-13T21:01:11
set clock timezone Europe/London
set clock ntp none
JS>set clock timezone Europe/Paris
JS>apply
JS>show clock
set clock timenow 2003-08-13T22:01:22
set clock timezone Europe/Paris
set clock ntp none
```

set clock ntp

Synopsis: `set clock ntp <IPLIST|none>`

A DDoS secure appliance unit can also take advantage of an NTP server to help maintain a more accurate value for the time. The `set clock ntp` command can be used to define one or more NTP servers to be used for synchronizing the time. Time synchronizations are performed every hour but if the difference between the DDoS secure appliance local clock and the NTP server clock is greater than a few minutes it is recommended that the `set clock timenow` command is used first to bring the two clocks closer together.

Example:

```
JS>set clock ntp 128.118.25.3,140.162.8.25,130.88.200.98
```

show timezones

Copyright © 2013, Juniper Networks, Inc

Synopsis: `show timezones`

It is possible to show a complete list of timezones supported by the appliance with the `show timezones` command. Since the list is quite long, the system automatic paging takes over before the first line of the answer scrolls off the top of the display. It is important to note that time zone values are case sensitive.

Example:

```
JS>show timezones
Available timezones:
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
Africa/Asmera
Africa/Bamako
Africa/Bangui
Africa/Banjul
Africa/Bissau
Africa/Blantyre
Africa/Brazzaville
Africa/Bujumbura
Africa/Cairo
Africa/Casablanca
 -- more –
```

Remote Alerts, Reports and Logging

DDoS secure appliance currently supports a number of methods for remote alerts, reports, and logs. Incident alerts can be sent remotely either via SNMP traps, or through email. Daily reports can also be sent remotely by email. Additionally, continuous log data can be sent to a remote syslog server, Webtrends server or NetFlow collector.

This section describes how to configure the specific settings needed to enable the above forms of remote messaging. This section does not, however, cover the configuration of event triggers that would then result in incident logs or alerts. These associated settings are covered in the Logging Threshold section.

The following sub-sections describe configuration for each of these remote messaging options.

SNMP

The SNMP protocol can be used with DDoS secure appliance to request data as well as send alerts. Thus, SNMP query related settings are also covered here. The same commands are used to manage settings that affect both SNMP alerts and queries.

Table 27: SNMP Parameters

PARAMETER	VALUE	DESCRIPTION
trap	IPLIST|none	The IP address(es) to which SNMP traps are sent
rocommunity	COMMUNITY	The community name required for read-only access to the SNMP variables.
trapcommunity	Community	The community name used when sending SNMP traps.
syslocation	TEXT	A description of the location of the DDoS secure appliance unit.

Copyright © 2013, Juniper Networks, Inc

syscontact	TEXT	Who to contact about the DDoS secure appliance unit.

show snmp

Synopsis: `show snmp`

Displays the current SNMP settings: the trap destination address, the read-only community string, the trap community string, the system location reference name, and the contact information for the system administrator.

Example:

```
JS>show snmp
set snmp trap 192.168.1.15 rocommunity public trapcommunity trapcom \
   syslocation test-lab    syscontact support@DDoS secure appliance-technology.com
```

set snmp

Synopsis: `set snmp [trap <IPLIST|none>] \`
`[rocommunity <COMMUNITY>] [trapcommunity <COMMUNITY>] \`
`[syslocation <TEXT>] [syscontact <TEXT>]`

The set snmp command is used to adjust the values of the SNMP trap address trap, the read only community string rocommunity, , the snmp community string trapcommunity,the system location string syslocation, and the system admin contact syscontact.

Example:

```
JS>show snmp
set snmp trap 192.168.1.15 rocommunity public trapcommunity public \
   syslocation test-lab    syscontact support@DDoS secure appliance-technology.com
JS>set snmp syslocation "DDoS secure appliance test lab"
JS>apply
JS>show snmp
set snmp trap 192.168.1.15 rocommunity public trapcommunity public \
   syslocation "DDoS secure appliance test lab" syscontact support@DDoS secure appliance-
technology.com
```

NOTE: Although `set snmp` allows the changing of both SNMP remote alerting and SNMP querying related settings, it does not change the security access settings to the DDoS secure appliance Management interface. It is important that the `set access snmp` command also be used to ensure that trusted IP addresses have access to the DDoS secure appliance if they are to be allowed to make SNMP queries.

Syslog

The syslog protocol is based on the message logging system of the same name (see RFC3164 The BSD syslog protocol). A DDoS secure appliance unit can be configured to send copies of messages that it records in its local log files to a remote syslog server.

Table 28: Syslog Parameters

PARAMETER	VALUE	DESCRIPTION
ip	IPLIST|none	The IP address (es) to which syslog messages will be sent.

Copyright © 2013, Juniper Networks, Inc

facility	SYSFACILITY	The syslog facility to which messages will be sent. If no previous facility has been defined and this parameter is not specified then the default daemon facility will be used.
priority	SYSPRIORITY	The syslog priority at or above appropriate messages will be sent. If no previous priority has been defined and this parameter is not specified then the default info priority will be used.

show syslog

Synopsis: `show syslog`

Displays the current syslog configuration.

Example:

```
JS>show syslog
set syslog ip 192.168.1.15 facility local5 priority info
```

set syslog

Synopsis: `set syslog [ip <IPLIST|none>] [facility <SYSFACILITY>] \ [priority <SYSPRIORITY>]`

DDoS secure appliance has three syslog configuration settings, but the only one that must be configured for messages to be sent is the IP address of the remote syslog server.

DDoS secure appliance will send syslog messages that are written into the log file that are at priority or higher.

Example:

```
JS>set syslog ip 192.168.0.10
JS>apply
JS>show syslog
set syslog ip 192.168.0.10 facility daemon priority info
```

Webtrends

The Webtrends Firewall Suite (WFS) supports the Webtrends Enhanced Logging Format (WELF) used with the syslog protocol. A DDoS secure appliance unit can be configured to log incident events in a WELF compatible format for collection and reporting by tools such as WFS. The logging configuration of Webtrends is the same as for syslog, except that any values used should be in accordance with the guidance given with a WFS or WELF compatible processing server. In particular, some Unix syslog servers are not able to keep up with the bursts of information often generated.

Table 29: Webtrends Parameters

PARAMETER	VALUE	DESCRIPTION
ip	IPLIST|none	The IP address to which Webtrends messages will be sent.
facility	SYSFACILITY	The syslog facility to which messages will be sent. If no previous facility has been defined and this parameter is not specified then the default daemon facility will be used.

Copyright © 2013, Juniper Networks, Inc

priority	SYSPRIORITY	The syslog priority with which messages will be sent. If no previous priority has been defined and this parameter is not specified then the default warn priority will be used.

show webtrends

Synopsis: `show webtrends`

Displays the current Webtrends logging configuration.

Example:

```
JS>show webtrends
set webtrends ip 192.168.1.99 facility local0 priority warn
```

set webtrends

Synopsis: `set webtrends [ip <IPLIST|none>] \`
`[facility <SYSFACILITY>] [priority <SYSPRIORITY>]`

Webtrends configuration is handled in the same way as ordinary syslog configuration.

NetFlow

The DDoS secure appliance is capable of sending NetFlow packets (Version 9: RFC 3954) to a NetFlow Collector for data analysis and reporting.

Table 30: NetFlow Parameters

PARAMETER	VALUE	DESCRIPTION
ip	IPLIST|IPMULTI|none	The IP address to which Webtrends messages will be sent.
port	PORT	The port number that the NetFlow Collector is listening on.
templatep	TEMPLATEP	Retransmit the NetFlow Templates after transmitting this number of NetFlow packets, or the templatem timeout has expired.
templatem	TEMPLATEM	Retransmit the NetFlow Templates after this time in minutes, or when templatep packets have been transmitted.
flowflush	FLOWFLUSH	Generate a NetFlow record for a flow after this time in minutes.

show netflow

Synopsis: `show netflow`

Displays the current NetFlow logging configuration.

Example:

```
JS>show netflow
set netflow ip 192.168.1.99 port 9996 templatep 1000 templatem 60 flowflush 1
```

set netflow

Synopsis: `set netflow [ip <IPLIST|IPMULTI|none>] [port <PORT>] \`
`[templatep <TEMPLATEP>] [templatem <TEMPLATEM>] \`
`[flowflush <FLOWFLUSH>]`

Copyright © 2013, Juniper Networks, Inc

The NetFlow Collector has to be configured to listen on the correct port, and the DDoS secure appliance IP address has to be configured as a valid source address.

Proxy Server

If the DDoS secure appliance needs to get update information via a URL, then the http traffic may have to go via a proxy server to get to the Internet.

Table 31: Proxy Server Parameters

PARAMETER	VALUE	DESCRIPTION
proxyip	IPADDRESS|none	The IP of the Proxy Server.
proxyport	PORT	The port number that the Proxy Server is listening on.
proxyuser	USERNAME|none	The user for authenticating to the Proxy Server
proxypassword	PASSWORD	The password for the user for authenticating to the Proxy Server.

show proxy

Synopsis: `show proxy`

Displays the current Proxy Server configuration.

Example:

```
JS>show proxy
set proxy ip 192.168.1.99 proxyport 8080 proxyuser "" proxypassword ""
```

set proxy

Synopsis: `set proxy [proxyip <IPADDRESS|none>] [proxyport <PORT>] \ [proxyuser <USERNAME|none>] [proxypassword <PASSWORD>]`

Mail Reporting

A DDoS secure appliance unit can send incident alerts, or daily-generated reports via email. These are configurable on a per portal basis.

Table 32: Mail Parameters

PARAMETER	VALUE	DESCRIPTION
to	EMAILADDRESSES	The email address to which the alert or daily report is to be sent. Comma separated addresses can be specified.
from	EMAILADDRESS	The email address from which the alert or daily report appears to come from.
server	IPADDRESS|none	The IP address of the SMTP server to which the alert or daily report is to be forwarded.

Copyright © 2013, Juniper Networks, Inc

wsserver	IPADDRESS|none	The IP address via which the DDoS secure appliance is accessed, which may be different to the actual DDoS secure appliance management IP address.
dailystats	yes|no	If set, a daily summary of statistics is emailed.
weeklystats	yes|no	If set, a weekly summary of statistics is emailed.
monthlystats	yes|no	If set, a monthly summary of statistics is emailed.
cluster	yes|no	If set, a cluster daily summary is sent out as well.
alerts	yes|no	If set, incident alerts are emailed out at a rate no faster than specified by alert interval.
alertinterval	ALERTINTERVAL	This is the minimum amount of time (in minutes) between two email alerts, acting as a rate limiter. Each email can contain information about multiple incidents.

show mail

Synopsis: `show mail`

Displays the current daily email configuration.

Example:

```
JS>show mail
set mail server 192.168.1.15 from ddos-secure@somewhere.com \
to somewhere@somewhere.com \
dailystats yes weeklystats yes monthlystats yes cluster no alerts no alertinterval 5
```

set mail

Synopsis: `set mail [to <EMAILADDRESSES>] [from <EMAILADDRESS>] \`
`[server <IPADDRESS|none>] [wsserver <IPADDRESS|none>] \`
`[dailystats <yes|no>] [weeklystats <yes|no>] \`
`[monthlystats <yes|no>] [alerts <yes|no>] \`
`[cluster <yes|no>] [alertinterval <ALERTINTERVAL>]`

Email will not be sent unless all parameter values (except wsserver) are defined. Below is an example warning given when only a server IP address has been configured. The configuration will still be accepted, but no email will be sent until the missing parameter values have been defined.

Example:

```
JS>set mail server 192.168.0.10
Warning: mail needs "to" parameter
Warning: mail needs "from" parameter
JS>apply
JS>show mail
set mail server 192.168.0.10
JS>
```


Copyright © 2013, Juniper Networks, Inc

Once a parameter value has been set, that value will be used until changed. It is not necessary to set all the values each time one of them needs to be changed. The server address can be set to `none` to disable emails from being sent.

Logging Thresholds

DDoS secure appliance uses a set of values known as Create Thresholds to determine the rate, for each defense type, at which the user would like an incident record to be created. The thresholds define at what rate packets must be dropped before the incident is created. An incident is considered closed when the drop rate remains below the defined threshold for more than the specified incident timeout.

The Create Thresholds are mirrored by three other sets of thresholds. The first of these is the Offenders Threshold set, which determine the rate at which packets must be dropped for an individual client IP address to warrant addition to the Worst Offenders table. The second set is the Alert Thresholds, which determine when an alert email or snmp trap is sent, as well as being logged into the regular log file. The third set is the View Thresholds, which determine the rates at which packets must be dropped before the corresponding incidents are listed on the Web User Interface. This last set is effectively a viewing filter to limit the display of incidents to those of most interest.

The commands in this section describe how to examine and change these threshold values, as well as ignore certain types of attack completely if desired.

Table 33: Logging Threshold Types

PARAMETER	DESCRIPTION
create	Thresholds associated with the creation of incidents
offenders	Thresholds associated with entry into the worst offenders table
alert	Thresholds associated with the sending of email alerts.
view	Thresholds associated with the viewing/display of incidents

The following tables describe the Logging Threshold parameters and their formats.

Table 34: Logging Threshold Parameters

PARAMETER	VALUE	DESCRIPTION
bandwidthenable	yes|no	Enable/disable logging dropped packets exceeding bandwidth threshold.
bandwidthrate	THRESHOLD	Threshold for logging dropped packets exceeding bandwidth threshold.
packetrateenable	yes|no	Enable/disable logging dropped packet rate packets.
packetraterate	THRESHOLD	Threshold for logging dropped packet rate packets.

Copyright © 2013, Juniper Networks, Inc

blockedprotocolenable	yes|no	Enable/disable logging dropped packets which do not match the appropriate filter.
blockedprotocolrate	THRESHOLD	Threshold for logging dropped packets which do not match the appropriate filter.
blockedstateenable	yes|no	Enable/disable logging dropped packets because they were out of state.
blockedstaterate	THRESHOLD	Threshold for logging dropped packets because they were out of state.
attackipenable	yes|no	Enable/disable logging dropped packets because they constitute an IP attack.
attackiprate	THRESHOLD	Threshold for logging dropped packets because they constitute an IP attack.
attacktcpenable	yes|no	Enable/disable logging dropped packets because they constitute a TCP attack.
attacktcprate	THRESHOLD	Threshold for logging dropped packets because they constitute a TCP attack.
attackudpenable	yes|no	Enable/disable logging dropped packets because they constitute a UDP attack.
attackudprate	THRESHOLD	Threshold for logging dropped packets because they constitute a UDP attack.
attackicmpenable	yes|no	Enable/disable logging dropped packets because they constitute an ICMP attack.
attackicmprate	THRESHOLD	Threshold for logging dropped packets because they constitute an ICMP attack.
attackotheripenable	yes|no	Enable/disable logging dropped packets because they constitute an attack not covered by the above 4 cases.
attackotheriprate	THRESHOLD	Threshold for logging dropped packets because they constitute an attack not covered by the above 4 cases.
attackfragmentenable	yes|no	Enable/disable logging dropped packets because they constitute a fragment attack.
attackfragmentrate	THRESHOLD	Threshold for logging dropped packets because they constitute a fragment attack.

Copyright © 2013, Juniper Networks, Inc

badippacketenable	yes|no	Enable/disable logging dropped packets because they are an invalid IP packet.
badippacketrate	THRESHOLD	Threshold for logging dropped packets because they are an invalid IP packet.
badtcppacketenable	yes|no	Enable/disable logging dropped packets because they are an invalid TCP packet.
badtcppacketrate	THRESHOLD	Threshold for logging dropped packets because they are an invalid TCP packet.
badudppacketenable	yes|no	Enable/disable logging dropped packets because they are an invalid UDP packet.
badudppacketrate	THRESHOLD	Threshold for logging dropped packets because they are an invalid UDP packet.
badicmppacketenable	yes|no	Enable/disable logging dropped packets because they are an invalid ICMP packet.
badicmppacketrate	THRESHOLD	Threshold for logging dropped packets because they are an invalid ICMP packet.
badotherippacketenable	yes|no	Enable/disable logging dropped packets because they are invalid and not covered by ip, tcp, udp and icmp cases.
badotherippacketrate	THRESHOLD	Threshold for logging dropped packets because they are invalid and not covered by ip, tcp, udp and icmp cases.
overloadedipenable	yes|no	Enable/disable logging packets because of the overloaded ip condition.
overloadediprate	THRESHOLD	Threshold for logging packets because of the overloaded ip condition.
allenable	yes|no	Enable/disable logging dropped packets for all attack types. This is a quick way of enabling or disabling everything.
allrate	THRESHOLD	Sets the threshold for logging all attack packets to be the same.
autoadjust	yes|no	Enable/disable automatic adjusting of create thresholds, so that the number of generated incidents per day is limited to being between 10 and 100 per type per day. Note: Only valid for **create**.

Copyright © 2013, Juniper Networks, Inc

show threshold view

Synopsis: `show threshold view`

Displays the current incident View Threshold configuration.

Example:

```
JS>show threshold view
set threshold view bandwidthenable yes bandwidthrate 100
set threshold view packetrateenable yes packetraterate 100
set threshold view blockedprotocolenable yes blockedprotocolrate 100
set threshold view blockedstateenable yes blockedstaterate 100
set threshold view attackipenable yes attackiprate 100
set threshold view attacktcpenable yes attacktcprate 100
set threshold view attackudpenable yes attackudprate 100
set threshold view attackicmpenable yes attackicmprate 100
set threshold view attackotheripenable yes attackotheriprate 100
set threshold view attackfragmentenable yes attackfragmentrate 100
set threshold view badippacketenable yes badippacketrate 100
set threshold view badtcppacketenable yes badtcppacketrate 100
set threshold view badudppacketenable yes badudppacketrate 100
set threshold view badicmppacketenable yes badicmppacketrate 100
set threshold view badotherippacketenable yes badotherippacketrate 100
set threshold view overloadedipenable yes overloadediprate 100
```

show threshold create

Synopsis: `show threshold create`

Displays the current incident Create Threshold configuration.

Example:

```
JS>show threshold create
set threshold create autoadjust yes
set threshold create bandwidthenable yes bandwidthrate 10
set threshold create packetrateenable yes packetraterate 10
set threshold create blockedprotocolenable yes blockedprotocolrate 10
set threshold create blockedstateenable yes blockedstaterate 10
set threshold create attackipenable yes attackiprate 10
set threshold create attacktcpenable yes attacktcprate 10
set threshold create attackudpenable yes attackudprate 10
set threshold create attackicmpenable yes attackicmprate 10
set threshold create attackotheripenable yes attackotheriprate 10
set threshold create attackfragmentenable yes attackfragmentrate 10
set threshold create badippacketenable yes badippacketrate 10
set threshold create badtcppacketenable yes badtcppacketrate 10
set threshold create badudppacketenable yes badudppacketrate 10
set threshold create badicmppacketenable yes badicmppacketrate 10
set threshold create badotherippacketenable yes badotherippacketrate 10
set threshold create overloadedipenable yes overloadediprate 10
```

show threshold offenders

Synopsis: `show threshold offenders`

Displays the Worst Offenders recording thresholds.

Example:

```
JS>show threshold offenders
set threshold offenders bandwidthenable yes bandwidthrate 10
```


Copyright © 2013, Juniper Networks, Inc

```
set threshold offenders packetrateenable yes packetraterate 10
set threshold offenders blockedprotocolenable yes blockedprotocolrate 10
set threshold offenders blockedstateenable yes blockedstaterate 10
set threshold offenders attackipenable yes attackiprate 10
set threshold offenders attacktcpenable yes attacktcprate 10
set threshold offenders attackudpenable yes attackudprate 10
set threshold offenders attackicmpenable yes attackicmprate 10
set threshold offenders attackotheripenable yes attackotheriprate 10
set threshold offenders attackfragmentenable yes attackfragmentrate 10
set threshold offenders badippacketenable yes badippacketrate 10
set threshold offenders badtcppacketenable yes badtcppacketrate 10
set threshold offenders badudppacketenable yes badudppacketrate 10
set threshold offenders badicmppacketenable yes badicmppacketrate 10
set threshold offenders badotherippacketenable yes badotherippacketrate 10
set threshold offenders overloadedipenable no overloadediprate 10
```

show threshold alert

Synopsis: `show threshold alert`

Displays the current incident Alert Threshold configurations.

Example:

```
JS>show threshold alert
set threshold alert bandwidthenable yes bandwidthrate 100
set threshold alert packetrateenable yes packetraterate 100
set threshold alert blockedprotocolenable yes blockedprotocolrate 100
set threshold alert blockedstateenable yes blockedstaterate 100
set threshold alert attackipenable yes attackiprate 100
set threshold alert attacktcpenable yes attacktcprate 100
set threshold alert attackudpenable yes attackudprate 100
set threshold alert attackicmpenable yes attackicmprate 100
set threshold alert attackotheripenable yes attackotheriprate 100
set threshold alert attackfragmentenable yes attackfragmentrate 100
set threshold alert badippacketenable yes badippacketrate 100
set threshold alert badtcppacketenable yes badtcppacketrate 100
set threshold alert badudppacketenable yes badudppacketrate 100
set threshold alert badicmppacketenable yes badicmppacketrate 100
set threshold alert badotherippacketenable yes badotherippacketrate 100
set threshold alert overloadedipenable no overloadediprate 100
```

set threshold

Synopsis: `set threshold <create|view|alert|offenders> \`
`<`*`PARAMETER`*`> <`*`VALUE`*`> […]`

The <*PARAMETER*> <*VALUE*> pair are taken from the Logging Threshold parameters table above.

The threshold is the number of packets dropped per second while the attack is in progress. Once this threshold rate is exceeded then the attack is logged as an incident. Create rates are calculated on a per protected server basis. The offenders rates are calculated on a per client basis.

NOTE: If view/alert threshold is set lower than the create threshold for a particular defense type, then it will only trigger when the Incident has been created.

show incidents

Synopsis: `show incidents`

Copyright © 2013, Juniper Networks, Inc

Displays the incident timeout, lifetime and warning threshold. An incident is closed when the packet rate has been below the create threshold for the specified number of timeout minutes, or the incident has been open for more than the specified lifetime minutes.

An Incident is only alerted on if the Incident has been above the Alert threshold for at least threshold seconds.

Example:

```
JS>show incidents
set incidents timeout 5 lifetime 60 threshold 60
```

Table 35: Incident Parameters

PARAMETER	VALUE	DESCRIPTION
timeout	TIMEOUT	How long an incident drop rate must be below the create threshold before the incident is closed (in minutes).
lifetime	LIFETIME	How long an Incident can live for (in minutes).
threshold	THRESHOLDTIME	Length of time an item is above the threshold before an event triggers (in seconds).

set incidents

Synopsis: `set incidents [timeout <TIMEOUT>] [lifetime <LIFETIME>] \ [threshold <THRESHOLDTTIME>]`

Sets the incident timeout, lifetime or threshold times.

Debug Options

The debug options are used to aid in the diagnosis of suspicious traffic handling by a DDoS secure appliance unit. When enabled, the DDoS secure appliance generates detailed logs, but this can be at the expense of top end performance. The debug options should only be enabled at the suggestion of DDoS secure appliance support staff. By default, `worstoffenders` and `autoblacklist` are enabled as they tend not to create too high a loading.

The following tables describe the Debug Option parameters and their formats.

Table 36: Debug Option Parameters

PARAMETER	VALUE	DESCRIPTION
bandwidth	yes|no	Bandwidth throttle debugging.
packetrate	yes|no	Packet Rate debugging.
blockedprotocol	yes|no	Blocked protocol debugging.
blockedstate	yes|no	Blocked state debugging.
attackip	yes|no	IP attack debugging.

Copyright © 2013, Juniper Networks, Inc

attacktcp	yes|no	TCP attack debugging.
attackudp	yes|no	UDP attack debugging.
attackicmp	yes|no	ICMP attack debugging.
attackotherip	yes|no	Other IP attack debugging.
attackfragment	yes|no	Fragment attack debugging.
badippacket	yes|no	Bad IP packet debugging.
badtcppacket	yes|no	Bad TCP packet debugging.
badudppacket	yes|no	Bad UDP packet debugging.
badicmppacket	yes|no	Bad ICMP packet debugging.
badotherippacket	yes|no	Bad other IP packet debugging.
serverstalloverload	yes|no	Server stall debugging.
all	yes|no	This is a special option and represents the combination of all the above combinations. Setting all to yes for example will set bandwidth, packetrate, etc. to yes which saves a lot of typing.
worstoffenders	yes|no	Log Worst Offenders to main log file
autoblacklist	yes|no	Log Auto-Black-List to main log file

show debugging

Synopsis: `show debugging`

Displays the current debugging options.

Example:

```
JS>show debugging
set debugging bandwidth yes packetrate no blockedprotocol no blockedstate no \
       attackip yes attacktcp no attackudp no attackicmp no attackotherip no \
       attackfragment no badippacket no badtcppacket no badudppacket no \
       badicmppacket no badotherippacket no serveroverload no worstoffenders yes \
   autoblacklist yes
```

set debugging

Synopsis: `set debugging` <*PARAMETER*> <*VALUE*> […]

The <*PARAMETER*> <*VALUE*> pair are taken from the Debug Option parameters table above.

Traffic Interception

Traffic Interception Modification

Copyright © 2013, Juniper Networks, Inc

The DDoS secure appliance has the ability to generate pages that can be served back to the requesting client if the traffic would otherwise be dropped by a DDoS secure appliance filter. For further information on how to configure these, see subsequent chapters in this document.

It is also possible to reverse the direction sense for specific VLANs where the notion of Internet and protected have to be reversed due to the network routing.

Table 37: Traffic Interception Parameters

PARAMETER	VALUE	DESCRIPTION
enable	yes|no	Enable/disable response page generation.
respcode	CODE	HTTP Response code to be generated
http_ports	PORTLIST|none	HTTP response on these ports only
https_ports	PORTLIST|none	HTTPS response on these ports only
vlan	VLAN	Operate on this VLAN

show wrapper

Synopsis: `show wrapper <all|blocked|reverse>`

Displays the current wrapping configuration.

Example:

```
JS>show wrapper all
set wrapper blocked country enable yes respcode 200 http_ports 80 https_ports none
set wrapper blocked ip enable yes respcode 200 http_ports 80 https_ports none
```

set wrapper blocked

Synopsis: `set wrapper blocked country enable <yes|no> \`
`http_ports <`*`PORTLIST`*`|none> htps_ports <`*`PORTLIST`*`|none>`

`set wrapper blocked ip enable <yes|no> \`
`http_ports <`*`PORTLIST`*`|none> htps_ports <`*`PORTLIST`*`|none>`

set wrapper reverse

`set wrapper reverse vlan <`*`VLAN`*`>`

This sets the traffic that match the specific VLAN tag to be treated as if flowing in the opposite direction.

Chassis Definitions

One version of the DDoS secure appliance is provided in a Chassis configuration with multiple blades where each blade is effectively a DDoS secure appliance is its own rights, but can share a common VIP for management access. Associated with this is the ability to configure the DDoS secure appliance as a BGP trigger router for re-routing of traffic.

Table 38: Chassis Parameters

Copyright © 2013, Juniper Networks, Inc

PARAMETER	VALUE	DESCRIPTION
ip	IPADDRESS	IP address to be used
netmask	NETMASK	Netmask to be used
ddos_secure	IPADDRESS	DDoS secure appliance blade acting as trigger router
our_as	ASNUMBER	Local AS #
neigh_ip	IPADDRESS	BGP neighbor router
neigh_as	ASNUMBER	Neighbor AS #
neigh_pass	PASSWORD	Password to secure communications with neighbor
comm_as	ASNUMBER	Trigger community AS #
comm_no	NUMBER	Trigger community number
lowertimer	NUMBER	Length of time below re-routing rate before dropping the trigger route

show chassis

Synopsis: `show chassis <all|vip|blade|bgp|reroute>`

Displays the current chassis configuration.

Example:

```
JS>show chassis all
set chassis blade ip 192.168.0.6
```

set chassis vip

Synopsis: `set chassis vip ip <IPADDRESS> netmask <NETMASK>`

Used to define the common VIP by which the DDoS secure appliance chassis can be accessed.

set chassis blade

Synopsis: `set chassis blade ip <IPADDRESS>`

Used to define the management access for the individual blade within the chassis. This is also used to define the IP addresses of DDoS secure appliances that are participating in BGP re-routing.

set chassis bgp

Synopsis:
```
set chassis bgp DDoS secure appliance <IPADDRESS> \
our_as <ASNUMBER>\
neigh_ip <IPADDRESS> neigh_as <ASNUMBER>\
neigh_pass <PASSWORD> comm_as <ASNUMBER>\
comm_no <NUMBER> lowertimer <NUMBER>
```

Copyright © 2013, Juniper Networks, Inc

Used to define the BGP setup where the defined DDoS secure appliance is going to act as a Trigger Router for injecting BGP routes. This is used in conjunction with the reroute definitions for a Portal which are applied on a per protected IP basis to inject or withdraw a route.

set chassis reroute

Synopsis: `set chassis reroute ip <IPADDRESS>`

Use of this forces a permanent injection of the defined protected IP into the BGP Trigger routing tables.

Copyright © 2013, Juniper Networks, Inc

CHAPTER 3

SYSTEM MAINTENANCE

This chapter describes the available system commands.

System Commands

system restart

Synopsis: `system restart`

Restarts the DDoS secure appliance software but does not restart the underlying operating system.

system restart_clear

Synopsis: `system restart_clear`

Restarts the DDoS secure appliance software but does not restart the underlying operating system. All tables aer cleared out, so the DDoS Secure appliance will need to re-learn everything.

system shutdown

Synopsis: `system restart`

Shuts down the DDoS secure appliance engine only. The underlying O/S continues to run as does the GUI / CLI interface.

system reboot

Synopsis: `system reboot`

Reboots the DDoS secure appliance appliance.

system powerdown

Synopsis: `system powerdown`

Shuts down and powers off the DDoS secure appliance appliance.

system factoryreset

Synopsis: `system factoryreset`

Resets the DDoS secure appliance configuration back to the factory default. This includes things such as IP addresses of the Management Interface and defined users.

system clear_custom

Synopsis: `system clear_custom`

Removes any custom installed templates, certificates or images.

system check

Synopsis: `system check`

Outputs a build and health check summary..

system helpdesk

Synopsis: `system helpdesk`

Copyright © 2013, Juniper Networks, Inc

Writes a copy of the HelpDesk file and the Dell DSET file to a formatted external USB Drive.

Copyright © 2013, Juniper Networks, Inc

CHAPTER 4

SETTINGS COMMAND LINE ENVIRONMENT

This chapter describes the settings for the CLI environment.

Terminal Configuration

The following tables describe the Terminal Configuration parameters and their formats.

Table 39: Terminal Configuration Parameters

PARAMETER	VALUE	DESCRIPTION
pause	*yes|no*	Enables or disables the automatic pause at the end of a screen of text. Disabling this feature can be useful in scripts to avoid the possibility of pauses which might interfere with the next line of the script. Default value is `yes`
confirmations	*yes|no*	Enables or disables confirmations. Disabling confirmations will stop the prompts— **are you sure**, from appearing. This can be useful in scripts. Default value is `yes`
lines	*LINES*	The number of vertical character lines the terminal is capable of displaying.
cols	*COLS*	The number of horizontal character columns the terminal is capable of displaying.
Term	*TERMTYPE*	The terminal type—e.g. vt220

how terminal

Synopsis: `show terminal`

Displays the current terminal settings for this session.

Example:

```
JS>show terminal
set terminal pause yes confirmations yes lines 24 cols 80 term vt100
```

set terminal

Synopsis: `set terminal [pause <yes|no>] [confirmations <yes|no>] \ [lines <LINES>] [cols <COLS>] [term <TERMTYPE>]`

Sets the terminal settings for the current CLI session. At the start of each new session the default values will be restored.

Copyright © 2013, Juniper Networks, Inc

Example:

```
JS>set terminal pause no confirmations no lines 24 cols 80
JS>apply
JS>show terminal
set terminal pause no confirmations no lines 24 cols 80 term vt100
```


Copyright © 2013, Juniper Networks, Inc

CHAPTER 5

STATISTICS AND INFORMATONAL COMMANDS

This chapter describes statistics and informational commands.

stats view

Synopsis: `stats view`

The `stats view` command will cause graphical, curses based, output to be displayed to the screen. Entering any key gives a list of all the available display options. The screen size and output format is based on terminal settings described in the previous section.

show version

Synopsis: `show version`

The `show version` command displays the current software release along with other version details about the unit.

Example:

```
JS>sh version
DDoS Secure Code Version:       5.13.1-2
DDoS Secure Code Base:          CENTOS_6_3
DDoS Secure Build Date:         201305201820GMT
CD Base Image:                  5.13.1-2
Actual Memory Size:             31.3G
Actual Number of CPUs:          16
Serial No:                      A1RYMW1
Hardware ID:                    90:B1:1C:2A:A3:28
Platform:                       J-DDOS-SEC-AP2
Last Restart:                   Tue May 21 16:54:09 2013
Licensed Throughput:            10G
Memory To Use:                  31G
CPUs To Use:                    16
Protected IPs Supported:        64K
Tracked IPs Supported:          32M
Portals Supported:              256
Filters Supported:              4K
MAC Entries Supported:          16K
TCP Entries Supported:          4M
UDP Entries Supported:          512K
ICMP Entries Supported:         64K
Other IP Entries Supported:     64K
Fragment Entries Supported:     32K
FTP Entries Supported:          8K
JS>
```

The following table describes the information of each line:

Copyright © 2013, Juniper Networks, Inc

Table 40: Show Version Parameters

PARAMETER	DESCRIPTION
DDoS Secure Code Version	The current version of the core DDoS Secure appliance software.
DDoS Secure Code Base	The underlying operating system
DDoS Secure Build Date	When the build took place
CD Base Image	The version of the CD used to re-image the unit.
Actual Memory Size	The unit's available RAM.
Actual Number of CPUs	The number of CPUs available.
Serial No	The Serial Number of the Appliance.
Hardware ID	The ID key of the Appliance.
Platform	The Juniper appliance model number.
Last Restart	The last time the DDoS Secure engine was restarted.
Licensed Throughput	This should match the size of the purchased License.
Memory To Use	Amount of memory the appliance is allowed to use.
CPUs To Use	Number of CPUs the appliance is allowed to use.
Protected IPs Supported	The maximum number of Protected IP addresses that can be tracked.
Tracked IPs Supported	The maximum number of Internet client IP address that can be tracked.
Portals Supported	The maximum number of Portals supported.
Filters Supported	The maximum number of Filters supported.
MAC Entries Supported	The maximum number of MAC entries supported.
TCP Entries Supported	The maximum number of TCP sessions supported.
UDP Entries Supported	The maximum number of UDP sessions supported.
ICMP Entries Supported	The maximum number of ICMP sessions supported.
Other IP Entries Supported	The maximum number of Other IP sessions supported.
Fragment Entries Supported	The maximum number of Fragment sessions supported.

Copyright © 2013, Juniper Networks, Inc

FTP Entries Supported	The maximum number of FTP sessions supported.

It is possible to update the “Supported” counts with the `set usage` command

Copyright © 2013, Juniper Networks, Inc

CHAPTER 6

BGP TRIGGER ROUTER CONFIGURATION

The DDoS Secure appliance can act as a trigger router in a Remote Triggered Black Hole (RTBH) environment. It is then down to the BGP environment as to whether any IPs re-routed by the trigger router is either null routed, or re-routed via some other infrastructure.

The code was initially created for the DDoS Secure appliancemitigation blade chassis - hence the CLI chassis syntax, where traffic can be re-routed via alternative blades. Something similar to the following 3 lines are needed to get BGP working, where A.B.C.D is your DDoS Secure appliance management IP address, and W.X.Y.Z is the peering BGP Router:-

```
JS> set chassis blade ip A.B.C.D
JS> set chassis bgp ddos_secure A.B.C.D our_as 65099 neigh_ip \
       W.X.Y.Z neigh_as 65014 neigh_pass 123456 \
       comm_as 65040 comm_no 99 lowertimer 300
JS> apply
```

This then generates a (quagga) config file on the DDoS Secure appliance which is similar to the following (ip prefix-list not-ours deny are the local DDoS Secure appliance IP addresses):

DDoS Secure appliance BGP Configuration

```
!
router bgp 65099
 bgp router-id A.B.C.D
 bgp log-neighbor-changes
 redistribute kernel route-map scrub-out
 redistribute static route-map scrub-out
 neighbor W.X.Y.Z remote-as 65014
 neighbor W.X.Y.Z password 123456
 neighbor W.X.Y.Z maximum-prefix 500
 neighbor W.X.Y.Z route-map scrub-out out
 neighbor W.X.Y.Z route-map scrub-in in
!
ip prefix-list not-ours seq 10 deny 1.1.1.128/30 le 32
ip prefix-list not-ours seq 20 deny 1.234.56.0/24 le 32
ip prefix-list not-ours seq 30 deny 169.254.0.0/16 le 32
ip prefix-list not-ours seq 40 deny 127.0.0.0/8 le 32
ip prefix-list not-ours seq 60 deny 192.168.0.0/24 le 32
ip prefix-list not-ours seq 70 deny 0.0.0.0/0
ip prefix-list not-ours seq 80 permit any
!
ip community-list 99 permit 65040:99
!
route-map scrub-out permit 10
 match ip address prefix-list not-ours
 set community 65040:99
!
route-map scrub-in deny 10
```


Copyright © 2013, Juniper Networks, Inc

Peering Router Sample Configuration

```
!
router bgp 65014
bgp log-neighbor-changes
neighbor A.B.C.D remote-as 65099
neighbor A.B.C.D password 123456
 !
address-family ipv4
  redistribute connected route-map internal
  redistribute static route-map internal
  neighbor A.B.C.D activate
  neighbor A.B.C.D send-community
  neighbor A.B.C.D route-map scrubbing in
  neighbor A.B.C.D route-map scrubbout out
  no auto-summary
  no synchronization
exit-address-family
!
ip bgp-community new-format
ip community-list 99 permit 65040:99
!
ip prefix-list localdeny seq 5 permit 10.10.10.1/32
!
ip prefix-list scrubb seq 5 permit F.G.H.0/21 le 32
!
route-map scrubbing permit 10
match ip address prefix-list scrubb
match community 99 exact-match
set local-preference 200
set community no-advertise
set ip next-hop W.X.Y.Z
!
route-map scrubbout permit 10
match ip address prefix-list localdeny
```

Re-Routing Trigger

These are based on the thresholds defined in the Portal Definition, and then applied to any IP address within that Portal.

The following table describes the 4 portal definitions that will be actioned if BGP is enabled:

Table 41: Re-routing Trigger Parameters

PARAMETER	DESCRIPTION
reroute**i**npkts	Packet rate has to remain below this threshold for at least `lowertimer` seconds for the routing trigger to be removed.
reroutemaxpkts	Packet rate threshold for routing trigger to be invoked
reroute**i**nspeed	Speed has to remain below this threshold for at least `lowertimer` seconds for the routing trigger to be removed
reroutemaxspeed	Speed threshold for routing trigger to be invoked

Copyright © 2013, Juniper Networks, Inc

Currently, only the protected IP is inserted as a trigger route.

Force Specific Re-Routing

To force any specific re-routing,

```
JS> set chassis reroute ip 1.2.3.4
JS> apply
```


Copyright © 2013, Juniper Networks, Inc

CHAPTER 7

BLOCKED COUNTRY RESPONSE CONFIGURATION

Before Configuration

If a packet is detected coming from a country that has been black-listed, the packet is simply dropped and recorded.

After Configuration

If a start of a new session packet comes from a country that is black-listed and is a web page request (to port 80, 443 or other optional ports), this is then redirected to an internal server that will serve up a content page indicating that access from this country is blocked, potentially giving a reason why and some contact information.This will allow the originator of the connection to request temporary access should they legitimately need it.

Content Presentation Information

File Naming

There are a series of template files named blockedcountryXXXXYYYYZZZZ.tmpl or blockedcountryXXXXYYYYZZZZ.tmpl, where:

- XXXX optionally can be -<DDoS Secure appliance Portal Name> where DDoS Secure appliance Portal Name is one of the optional user defined DDoS Secure appliance Portals.
- YYYY optionally can be -CCC where CCC is the 3 letter country code.
- ZZZZ optionally can be -www.domain.com.

The most specific match will be used with blockedcountryYYYY.tmpl overriding blockedcountryXXXX.tmpl.

File Content

The content will be standard html (<html> ….. </html>) with replaceable keywords.

NOTE: Any references to external (to the page) information (e.g. <img>, <frame>, href= etc.) should be used with care, as they cannot be hosted on any of the protected websites as access to the references will also get (recursively) blocked.

The following table describes keywords that can be recognized and replaced:

Table 42: File Content Parameters

PARAMETER	DESCRIPTION
%HOST%	Entry from the Host: Header

Copyright © 2013, Juniper Networks, Inc

%URL%	URL from the GET/POST/HEAD request. The Host: Header entry will be prefixed when appropriate.
%CCC%	Country Name
%IP%	Requesting IP
%TIME%	Current time of day (local time) in 'DAY MMM NNN HH:MM:SS YEAR' format (e.g. Wed Jun 30 21:49:08 1993).

Cache-Control will be set to `Cache-Control: no-cache, no-store` in the response headers.

The page must be no more than 1000 bytes, so that it (along with the headers) can be sent back in a single packet.

The connection will be closed after serving the content.

If templates are not added, or are not matched, the following built-in template is used

```
<html>
<h1>Access Administratively Blocked</h1>
<br>URL : '%URL%'
<br>Country : '%CCC%'
<br>Client IP address : '%IP%'
</html>
```

Intercept Server Information

This is a simple Webserver, running in a chroot, setuid environment on the DDoS Secure appliance. The blockedcountryXXXYYYYZZZZ.tmpl files will have the % keywords replaced at usage time.

The blockedcountryXXXYYYYZZZZ.tmpl files are updated through the DDoS Secure appliance GUI using the patch update mechanism. The patch update file (bc.upg) will (on a linux system) need to be built with the following command

```
echo 5.13 > webscreen- ; tar cvf bc.upg webscreen-
blockedcountry*.tmpl
```

To delete a .tmpl file, repeat the line above, but without the file in question and re-install the `bc.upg` patch.

This server will handle both http and https connections. For https connections, either a self-signed certificate or a CA signed certificate can be uploaded by including the file redirect.pem (which includes both the public and private key) in the bc.upg file.

DDoS Secure appliance Engine Configuration

This can only be done through the CLI interface. The commands are:

- `show wrapper all`
- `show wrapper blocked all`
- `remove wrapper blocked`
- `set wrapper blocked country enable <yes|no> respcode <resp code>\ http_ports <none|PORT> https_posts <none|PORT>`

Copyright © 2013, Juniper Networks, Inc

Testing

It is possible to re-classify the country code for any IP address.The testing process is:

- Select and Block a particular country (e.g –pr (RFC1918 addresses)）

  ```
  set block country –pr
  ```

- Reassign IP Address through the CLI.
  ```
  set geoip ip code –pr ip 1.2.3.4
  ```
- Test with connections from the IP 1.2.3.4 to get warning page.
- Add 1.2.3.4 to allow country block override list and verify that the normal page is reached.
  ```
  set block cignoreip 1.2.3.4
  ```

Reverse out configuration changes when finished.

NOTE: If the DDoS Secure appliance Engine is in Logging mode, then this warning page will not get generated as all traffic is passed through anyway – even if a country is blocked.

Country Block Bypass

Individual IP addresses, ranges or subnets can be configured to override Country Blocking so they are then allowed normal access, despite the traffic coming from a blocked country. This can be done through the GUI or CLI.

Copyright © 2013, Juniper Networks, Inc

APPENDIX A

DDOS SECURE APPLIANCE TCP STATES

The following denotes the TCP states held by DDoS Secure appliance during operation. These correspond approximately to the standard states held by a conventional TCP device, but are subdivided due to the unique method of handling connections by DDoS Secure appliance

The following table provides TCP status details.

Table 43: TCP Status Details

PARAMETER	DESCRIPTION
SYN	Client has sent a SYN.
SPF	Client has sent a SYN to an internally filtered port.
SIF	Client has sent a SYN to an internally filtered IP address.
S-A	Server has responded with SYN-ACK.
S-S	Client and server SYN.
ACK	Connection Established, but no data from Client or Server.
P-A	Client sent data, Server did not acknowledged any data.
GET	Currently processing an HTTP GET / HEAD / POST request.
EST	Connection established, data is flowing.
F1S	Internet has sent a FIN.
F2S	Protected ACKd FIN.
F3S	Internet sent FIN, protected ACKd FIN and has sent its own FIN.
F-F	Internet and protected sent FIN, but neither ACKd FIN.
F1D	Protected has sent a FIN.
F2D	Internet has ACKd FIN.
F3D	Protected sent FIN, Internet ACKd FIN and sent its own FIN.

Copyright © 2013, Juniper Networks, Inc

CLS	Closed (All FINs ACKd).
RST	RESET (either end) to SYN.
R-C	RESET (either end) to force session close.
UNK	Session in unknown state.
GETs	Count of connections processing a GET / HEAD request.

Copyright © 2013, Juniper Networks, Inc

APPENDIX B

ICMP TYPES

The following table provides ICMPv4 details.

Table 44: ICMPv4 Details

PARAMETER	DESCRIPTION
Echo Reply	0
Destination Unreachable	3
Source Quench	4
Redirect (change route)	5
Echo Request	8
Time Exceeded	11
Parameter Problem	12
Timestamp Request	13
Timestamp Reply	14
Information Request	15
Information Reply	16
Address Mask Request	17
Address Mask Reply	18

The following table provides ICMPv6 details.

Table 45: ICMPv6 Details

PARAMETER	DESCRIPTION
Destination Unreachable	1
Packet Too Big	2

Copyright © 2013, Juniper Networks, Inc

Time Exceeded	3
Parameter Problem	4
Echo Request	128
Echo Reply	129
Group Membership Query	130
Group Membership Reply	131
Group Membership Reduction	132
Router Solicitation	133
Router Advertisment	134
Neighbor Solicitation	135
Neighbor Advertisement	136
Redirect	137

Copyright © 2013, Juniper Networks, Inc

APPENDIX C

INCIDENT (ATTACK) TYPES

The following table provides type code details.

Table 46: Type Code Details

PARAMETER	DESCRIPTION
-2	Recorded in Auto-Black List.
-1	Packets not dropped, not recorded in Worst Offenders.
0	Not recorded in Worst Offenders.
1	Irritant attacks–used by Worst Offenders and Auto Black-List.
2	Resource consuming attacks–used by Worst Offenders and Auto Black-List.

The following table provides attack type code details.

Table 47: Attack Type Details

ATTACK TYPE	TYPE	DETAILS
Bad ICMP Packet–Malformed	1	ICMP header malformed (length, options and so on).
Bad IP Packet - Broken Header	1	IP header malformed–RFC non-compliant.
Bad IP Packet - Invalid Option	1	IP packet has invalid option field or field length.
Bad IP Packet - Invalid Source Address	0	IP packet has invalid source address.
Bad IP Packet - Reflected Route	-1	IP packet is being reflected off a router–same packet is passed both ways through the DDoS Secure appliance. Informational only.
Bad IP Packet - Size Mismatch	1	IP packet has invalid field length.
Bad O-IP Packet - Length	1	IP packet too short to contain IP Protocol header.
Bad O-IP Packet - Protocol	1	Invalid IP protocol number.
Bad TCP Packet - Fast Repeat Ack	0	Identical packets containing ACKs are being repeated a a rate of greater than 10 per second.

Copyright © 2013, Juniper Networks, Inc

Bad TCP Packet - Flags	1	Invalid TCP flag combinations.
Bad TCP Packet - Malformed	1	Format of TCP Header invalid.
Bad TCP Packet - Option	1	Invalid TCP option field.
Bad UDP Packet - Malformed	1	UDP header malformed.
Bad UDP Packet - No data	1	UDP packet contains no data.
Bandwidth	2	Bandwidth rate exceeded for MAC address / portal / Filter.
Blocked Protocol–AS Blocked	0	AS has been blocked.
Blocked Protocol–Black-Listed	0	This IP address has been black-listed as it is part of a black-listed network.
Blocked Protocol–Blocked DNS	1	DNS query has been blocked.
Blocked Protocol–Blocked URL	1	URL request has been blocked.
Blocked Protocol–Country Blocked	0	Traffic to / from Country has been blocked.
Blocked Protocol–Icmp Type	1	No filters match for this ICMP packet.
Blocked Protocol–Other Proto	1	No filters match for this protocol type.
Blocked Protocol–Port	1	No Filter match for this destination port.
Blocked Protocol–Temp Black-Listed	-2	This IP address has been temporarily black-listed.
Blocked Protocol–Undefined protected IP	0	Traffic to or from what is not defined as a protected IP address.
Fragment Attack–Bad Length	2	Invalid fragment length in IP header.
Fragment Attack–Header Overlay	2	Fragment start overlays protocol header.
Fragment Attack–No Fragments allowed	1	Fragmentation has been disabled in the Filter.
Fragment Attack–Ping of Death	2	Assembled packet is longer than 65535 bytes.
Fragment Attack–Repeats	1	Same fragment is resent.
Fragment Attack–Small Size	2	Initial TCP fragment is smaller than header.

Copyright © 2013, Juniper Networks, Inc

Fragment Attack–Table Full	1	Internal state table for fragments is full.
Fragment Attack–Timeout	2	Not all fragments seen.
ICMP Attack–Repeats	1	ICMP packets being repeated at a rate of more than 40 per second.
ICMP Attack–Table Full	1	Internal state table for ICMP is full.
IP Attack–Land	2	Source and destination IP addresses are equal.
Not Passed Thru–BPDU Packet	0	Fail-Over mode does not allow through Spanning Tree packets.
Not Passed Thru–Cripple State	0	Fail-Over is in Cripple state, no packets are being passed through.
Not Passed Thru–Deactivated	0	DDoS Secure appliance has operationally closed down.
Not Passed Thru–Direction Unknown	0	Logging-Tap only. MAC address not learnt yet.
Not Passed Thru–Generated Response	0	ARP Packet generated by redirect server.
Not Passed Thru–HeartBeat	0	Fail-Over heartbeat is never passed through a DDoS Secure appliance.
Not Passed Thru–Keep-Alive Response	0	TCP response packet to internally generated Keep-Alive probe packet has been dropped.
Not Passed Thru–MAC Misconfigured	0	A MAC address has been configured for one side of DDoS Secure appliance, but this packet with this source MAC address has been seen on the wrong side of the DDoS Secure appliance.
Not Passed Thru–MAC Table Overflow	0	Internal table for MAC addresses is full. Oldest entry has been expired.
Not Passed Thru–Packet From Us	0	Packet sent by someone pretending to be Internet or protected interface by using their MAC address.
Not Passed Thru–Packet To Us	0	Packet sent to Internet or protected interface MAC address.
Not Passed Thru–Pause Frame	0	Ethernet pause frame has been dropped.
Not Passed Thru–Probe State	0	Fail-Over is in Probe state, so no traffic passing through yet.

Copyright © 2013, Juniper Networks, Inc

Not Passed Thru–Runt Packet	0	Undersized packet has been dropped.
Not Passed Thru–Same Side	0	The source and destination MAC addresses both reside on the same side of the DDoS Secure appliance.
Not Passed Thru–Short Circuit Active	0	The same (source) MAC address has been seen on both sides of the DDoS Secure appliance.
Not Passed Thru–Standby State	0	Fail-Over is in Standby state–traffic flows through other DDoS Secure appliance.
Not Passed Thru–State Sync	0	State Synchronization packets are only processed.
Not Passed Thru–State Sync Sent	0	State Synchronization packets are only processed.
Other-IP Attack–Table Full	1	Internal state table for Other IP protocols is full.Oldest entry has been expired.
Overloaded IP–Backlog	1	The protected IP cannot keep up with new TCP connection requests.
Overloaded IP - Stall	1	The protected IP has stopped responding to anything.
Overloaded IP - Threads	2	The protected IP has stopped responding to new HTTP GET requests.
Packet Rate	2	Packet rate exceeded as defined in a filter or portal.
TCP Attack–Client Abort	1	Client aborted connection after request.
TCP Attack - Connection Flood	2	The protected IP has reached its concurrent connection configured limit.
TCP Attack - Connection Rate Flood	2	The protected IP is receiving connection requests at a rate higher than it is configured for.
TCP Attack - GET Flood	2	The protected IP has reached its concurrent GET/ HEAD configured limit.
TCP Attack - GET Incomplete	2	The HTTP GET request was never completed.
TCP Attack - GET Rate Flood	2	The protected IP is receiving GET requests at a rate higher than it is configured for.
TCP Attack - GET Timeout	1	The protected IP did not respond to a GET / HEAD request in a timely manner.

Copyright © 2013, Juniper Networks, Inc

TCP Attack - No Data Xfer	1	No data in either direction was transferred on the TCP connection. The connection was just opened and then closed.
TCP Attack - No Server Data Xfer	1	A web Server did not respond to a GET request. Usually seen when an IP addresses is requested in the Host: header field, instead of a domain name.
TCP Attack–Port Scan	2	A potential port scan was detected.
TCP Attack–RST	1	RST packet has invalid sequence number.
TCP Attack–Small Window	2	Client has closed TCP Window.
TCP Attack - Syn-Ack Timeout	2	The client IP did not complete the TCP connection.
TCP Attack - Syn Flood	2	The protected IP is receiving SYN packets at a rate higher than it is configured for or can handle.
TCP Attack - Table Full	1	Internal state table for TCP connections is full.
UDP Attack - Table Full	1	Internal state table for UDP information is full.
Unknown Session - Icmp Diag Response	1	ICMP diagnostic response packet does not match a state table entry for the respective IP protocol.
Unknown Session - Icmp Response	1	ICMP response packet has no matching ICMP request in state table.
Unknown Session - Invalid State	1	TCP packet has a state table entry, but packet is out of state (sequence numbers mismatch, or incorrect TCP flags).
Unknown Session - No State	1	TCP packet has no state table entry and is not a SYN (start of connection) packet.

Copyright © 2013, Juniper Networks, Inc

APPENDIX D

LETTER COUNTRY CODES

Sorted by Code

```
---: --Unknown—
-bc: ---Broadcast---        Cannot be Blocked
-bl: ---Black List---       Always is Blocked
-bo: ---Bogon Address---
-ca: ---Country Allow ---
-ce: ---Class E---
-dc: ---Default Charm---
-lo: ---Loopback---
-mc: ---Multicast---        Cannot be Blocked
-mp: ---Mega Proxy---       Cannot be Blocked
-nb: ---No Auto Block---
-pl: ---Preferred List---
-pr: ---RFC1918 Address---
-u1: ---User Defined #1---
-u2: ---User Defined #2---
-u3: ---User Defined #3---
-u4: ---User Defined #4---
-u5: ---User Defined #5---
-u6: ---User Defined #6---
-u7: ---User Defined #7---
-u8: ---User Defined #8---
-u9: ---User Defined #9---
-wl: ---White List---       Cannot be Blocked
-wn: ---White No Log---     Cannot be blocked
A1 : Anonymous Proxy
A2 : Satellite Provider
ABW: Aruba
AFG: Afghanistan
AGO: Angola
AIA: Anguilla
ALA: Aland Islands
ALB: Albania
AND: Andorra
ANT: Netherlands Antilles
AP : Asia/Pacific Region
AQ : Antarctica
ARE: United Arab Emirates
ARG: Argentina
ARM: Armenia
ASM: American Samoa
ATG: Antigua and Barbuda
AUS: Australia
AUT: Austria
AZE: Azerbaijan
BDI: Burundi
BEL: Belgium
BEN: Benin
BFA: Burkina Faso
BGD: Bangladesh
BGR: Bulgaria
BHR: Bahrain
BHS: Bahamas
BIH: Bosnia and Herzegovina
BLR: Belarus
BLZ: Belize
BMU: Bermuda
BOL: Bolivia
BRA: Brazil
BRB: Barbados
BRN: Brunei Darussalam
BTN: Bhutan
BV : Bouvet Island
BWA: Botswana
CAF: Central African Republic
CAN: Canada
CC : Cocos (Keeling) Islands
CHE: Switzerland
CHL: Chile
CHN: China
CIV: Cote DIvoire
CMR: Cameroon
COD: Congo, The Democratic Republic of the
COG: Congo
COK: Cook Islands
COL: Colombia
COM: Comoros
CPV: Cape Verde
CRI: Costa Rica
CUB: Cuba
CX : Christmas Island
CYM: Cayman Islands
CYP: Cyprus
CZE: Czech Republic
DEU: Germany
DJI: Djibouti
DMA: Dominica
DNK: Denmark
DOM: Dominican Republic
DZA: Algeria
ECU: Ecuador
EGY: Egypt
ERI: Eritrea
ESH: Western Sahara
ESP: Spain
EST: Estonia
ETH: Ethiopia
EU : Europe
FIN: Finland
FJI: Fiji
FLK: Falkland Islands (Malvinas)
FRA: France
FRO: Faroe Islands
FSM: Micronesia, Federated States of
FX : France, Metropolitan
GAB: Gabon
GBR: United Kingdom
GEO: Georgia
GGY: Guernsey
GHA: Ghana
GIB: Gibraltar
GIN: Guinea
GLP: Guadeloupe
GMB: Gambia
GNB: Guinea-Bissau
GNQ: Equatorial Guinea
GRC: Greece
GRD: Grenada
GRL: Greenland
GS : South Georgia and the South Sandwich Islands
GTM: Guatemala
GUF: French Guiana
GUM: Guam
GUY: Guyana
HKG: Hong Kong
HM : Heard Island and McDonald Islands
HND: Honduras
HRV: Croatia
HTI: Haiti
HUN: Hungary
```

Copyright © 2013, Juniper Networks, Inc

IDN: Indonesia
IMN: Isle of Man
IND: India
IO : British Indian Ocean Territory
IRL: Ireland
IRN: Iran, Islamic Republic of
IRQ: Iraq
ISL: Iceland
ISR: Israel
ITA: Italy
JAM: Jamaica
JEY: Jersey
JOR: Jordan
JPN: Japan
KAZ: Kazakhstan
KEN: Kenya
KGZ: Kyrgyzstan
KHM: Cambodia
KIR: Kiribati
KNA: Saint Kitts and Nevis
KOR: Korea, Republic of
KWT: Kuwait
LAO: Lao Peoples Democratic Republic
LBN: Lebanon
LBR: Liberia
LBY: Libyan Arab Jamahiriya
LCA: Saint Lucia
LIE: Liechtenstein
LKA: Sri Lanka
LSO: Lesotho
LTU: Lithuania
LUX: Luxembourg
LVA: Latvia
MAC: Macau
MAR: Morocco
MCO: Monaco
MDA: Moldova, Republic of
MDG: Madagascar
MDV: Maldives
MEX: Mexico
MHL: Marshall Islands
MKD: Macedonia
MLI: Mali
MLT: Malta
MMR: Myanmar
MNE: Montenegro
MNG: Mongolia
MNP: Northern Mariana Islands
MOZ: Mozambique
MRT: Mauritania
MSR: Montserrat
MTQ: Martinique
MUS: Mauritius
MWI: Malawi
MYS: Malaysia
NAM: Namibia
NCL: New Caledonia
NER: Niger
NFK: Norfolk Island
NGA: Nigeria
NIC: Nicaragua
NIU: Niue
NLD: Netherlands
NOR: Norway
NPL: Nepal
NRU: Nauru
NZL: New Zealand
O1 : Other
OMN: Oman
PAK: Pakistan
PAN: Panama
PCN: Pitcairn Islands
PER: Peru
PHL: Philippines
PLW: Palau
PNG: Papua New Guinea
POL: Poland
PRI: Puerto Rico
PRK: Korea, Democratic Peoples Republic of
PRT: Portugal
PRY: Paraguay
PSE: Palestinian Territory
PYF: French Polynesia
QAT: Qatar
REU: Reunion
ROU: Romania
RUS: Russian Federation
RWA: Rwanda
SAU: Saudi Arabia
SDN: Sudan
SEN: Senegal
SGP: Singapore
SHN: Saint Helena
SJM: Svalbard and Jan Mayen
SLB: Solomon Islands
SLE: Sierra Leone
SLV: El Salvador
SMR: San Marino
SOM: Somalia
SPM: Saint Pierre and Miquelon
SRB: Serbia
STP: Sao Tome and Principe
SUR: Suriname
SVK: Slovakia
SVN: Slovenia
SWE: Sweden
SWZ: Swaziland
SYC: Seychelles
SYR: Syrian Arab Republic
TCA: Turks and Caicos Islands
TCD: Chad
TF : French Southern Territories
TGO: Togo
THA: Thailand
TJK: Tajikistan
TKL: Tokelau
TKM: Turkmenistan
TLS: Timor-Leste
TON: Tonga
TTO: Trinidad and Tobago
TUN: Tunisia
TUR: Turkey
TUV: Tuvalu
TWN: Taiwan
TZA: Tanzania, United Republic of
UGA: Uganda
UKR: Ukraine
UM : United States Minor Outlying Islands
URY: Uruguay
USA: United States
UZB: Uzbekistan
VAT: Holy See (Vatican City State)
VCT: Saint Vincent and the Grenadines
VEN: Venezuela
VGB: Virgin Islands, British
VIR: Virgin Islands, U.S.
VNM: Vietnam
VUT: Vanuatu
WLF: Wallis and Futuna
WSM: Samoa
YEM: Yemen
YT : Mayotte

Copyright © 2013, Juniper Networks, Inc

```
ZAF: South Africa
ZMB: Zambia
ZWE: Zimbabwee
```

Sorted by Country

```
-bl: ---Black List---       Always is Blocked

-bo: ---Bogon Address---
-bc: ---Broadcast---        Cannot be Blocked
-ca: ---Country Allow---
-ce: ---Class E---
-dc: ---Default Charm---
-lo: ---Loopback---
-mc: ---Multicast---        Cannot be Blocked
-mp: ---Mega Proxy---       Cannot be Blocked
-nb: ---No Auto Block---
-pt: ---Pen Test List---
-pl: ---Preferred List---
-pr: ---RFC1918 Address---
-u1: ---User Defined #1---
-u2: ---User Defined #2---
-u3: ---User Defined #3---
-u4: ---User Defined #4---
-u5: ---User Defined #5---
-u6: ---User Defined #6---
-u7: ---User Defined #7---
-u8: ---User Defined #8---
-u9: ---User Defined #9---
-wl: ---White List---       Cannot be Blocked
-wn: ---White No Log---     Cannot be Blocked
---: --Unknown--
AFG: Afghanistan
ALA: Aland Islands
ALB: Albania
DZA: Algeria
ASM: American Samoa
AND: Andorra
AGO: Angola
AIA: Anguilla
A1 : Anonymous Proxy
AQ : Antarctica
ATG: Antigua and Barbuda
ARG: Argentina
ARM: Armenia
ABW: Aruba
AP : Asia/Pacific Region
AUS: Australia
AUT: Austria
AZE: Azerbaijan
BHS: Bahamas
BHR: Bahrain
BGD: Bangladesh
BRB: Barbados
BLR: Belarus
BEL: Belgium
BLZ: Belize
BEN: Benin
BMU: Bermuda
BTN: Bhutan
BOL: Bolivia
BIH: Bosnia and Herzegovina
BWA: Botswana
BV : Bouvet Island
BRA: Brazil
IO : British Indian Ocean Territory
BRN: Brunei Darussalam
BGR: Bulgaria
BFA: Burkina Faso
BDI: Burundi
KHM: Cambodia
CMR: Cameroon
CAN: Canada
CPV: Cape Verde
CYM: Cayman Islands
CAF: Central African Republic
TCD: Chad
CHL: Chile
CHN: China
CX : Christmas Island
CC : Cocos (Keeling) Islands
COL: Colombia
COM: Comoros
COG: Congo
COD: Congo, The Democratic Republic of the
COK: Cook Islands
CRI: Costa Rica
CIV: Cote DIvoire
HRV: Croatia
CUB: Cuba
CYP: Cyprus
CZE: Czech Republic
DNK: Denmark
DJI: Djibouti
DMA: Dominica
DOM: Dominican Republic
ECU: Ecuador
EGY: Egypt
SLV: El Salvador
GNQ: Equatorial Guinea
ERI: Eritrea
EST: Estonia
ETH: Ethiopia
EU : Europe
FLK: Falkland Islands (Malvinas)
FRO: Faroe Islands
FJI: Fiji
FIN: Finland
FRA: France
FX : France, Metropolitan
GUF: French Guiana
PYF: French Polynesia
TF : French Southern Territories
GAB: Gabon
GMB: Gambia
GEO: Georgia
DEU: Germany
GHA: Ghana
GIB: Gibraltar
GRC: Greece
GRL: Greenland
GRD: Grenada
GLP: Guadeloupe
GUM: Guam
GTM: Guatemala
GGY: Guernsey
GIN: Guinea
GNB: Guinea-Bissau
GUY: Guyana
HTI: Haiti
HM : Heard Island and McDonald Islands
VAT: Holy See (Vatican City State)
HND: Honduras
HKG: Hong Kong
HUN: Hungary
ISL: Iceland
IND: India
IDN: Indonesia
IRN: Iran, Islamic Republic of
IRQ: Iraq
IRL: Ireland
```

Copyright © 2013, Juniper Networks, Inc

IMN: Isle of Man
ISR: Israel
ITA: Italy
JAM: Jamaica
JPN: Japan
JEY: Jersey
JOR: Jordan
KAZ: Kazakhstan
KEN: Kenya
KIR: Kiribati
PRK: Korea, Democratic Peoples Republic of
KOR: Korea, Republic of
KWT: Kuwait
KGZ: Kyrgyzstan
LAO: Lao Peoples Democratic Republic
LVA: Latvia
LBN: Lebanon
LSO: Lesotho
LBR: Liberia
LBY: Libyan Arab Jamahiriya
LIE: Liechtenstein
LTU: Lithuania
LUX: Luxembourg
MAC: Macau
MKD: Macedonia
MDG: Madagascar
MWI: Malawi
MYS: Malaysia
MDV: Maldives
MLI: Mali
MLT: Malta
MHL: Marshall Islands
MTQ: Martinique
MRT: Mauritania
MUS: Mauritius
YT : Mayotte
MEX: Mexico
FSM: Micronesia, Federated States of
MDA: Moldova, Republic of
MCO: Monaco
MNG: Mongolia
MNE: Montenegro
MSR: Montserrat
MAR: Morocco
MOZ: Mozambique
MMR: Myanmar
NAM: Namibia
NRU: Nauru
NPL: Nepal
NLD: Netherlands
ANT: Netherlands Antilles
NCL: New Caledonia
NZL: New Zealand
NIC: Nicaragua
NER: Niger
NGA: Nigeria
NIU: Niue
NFK: Norfolk Island
MNP: Northern Mariana Islands
NOR: Norway
OMN: Oman
O1 : Other
PAK: Pakistan
PLW: Palau
PSE: Palestinian Territory
PAN: Panama
PNG: Papua New Guinea
PRY: Paraguay
PER: Peru
PHL: Philippines
PCN: Pitcairn Islands
POL: Poland
PRT: Portugal
PRI: Puerto Rico
QAT: Qatar
REU: Reunion
ROU: Romania
RUS: Russian Federation
RWA: Rwanda
SHN: Saint Helena
KNA: Saint Kitts and Nevis
LCA: Saint Lucia
SPM: Saint Pierre and Miquelon
VCT: Saint Vincent and the Grenadines
WSM: Samoa
SMR: San Marino
STP: Sao Tome and Principe
A2 : Satellite Provider
SAU: Saudi Arabia
SEN: Senegal
SRB: Serbia
SYC: Seychelles
SLE: Sierra Leone
SGP: Singapore
SVK: Slovakia
SVN: Slovenia
SLB: Solomon Islands
SOM: Somalia
ZAF: South Africa
GS : South Georgia and the South Sandwich Islands
ESP: Spain
LKA: Sri Lanka
SDN: Sudan
SUR: Suriname
SJM: Svalbard and Jan Mayen
SWZ: Swaziland
SWE: Sweden
CHE: Switzerland
SYR: Syrian Arab Republic
TWN: Taiwan
TJK: Tajikistan
TZA: Tanzania, United Republic of
THA: Thailand
TLS: Timor-Leste
TGO: Togo
TKL: Tokelau
TON: Tonga
TTO: Trinidad and Tobago
TUN: Tunisia
TUR: Turkey
TKM: Turkmenistan
TCA: Turks and Caicos Islands
TUV: Tuvalu
UGA: Uganda
UKR: Ukraine
ARE: United Arab Emirates
GBR: United Kingdom
USA: United States
UM : United States Minor Outlying Islands
URY: Uruguay
UZB: Uzbekistan
VUT: Vanuatu
VEN: Venezuela
VNM: Vietnam
VGB: Virgin Islands, British
VIR: Virgin Islands, U.S.
WLF: Wallis and Futuna
ESH: Western Sahara
YEM: Yemen
ZMB: Zambia
ZWE: Zimbabwe

Copyright © 2013, Juniper Networks, Inc

APPENDIX E

PANEL AND CONNECTOR LOCATIONS

DDoS Secure1200-FAILSAFE Panels

Figure 1 displays the front panel of DDoS Secure1200 Failsafe.

Figure 1: Front Panel

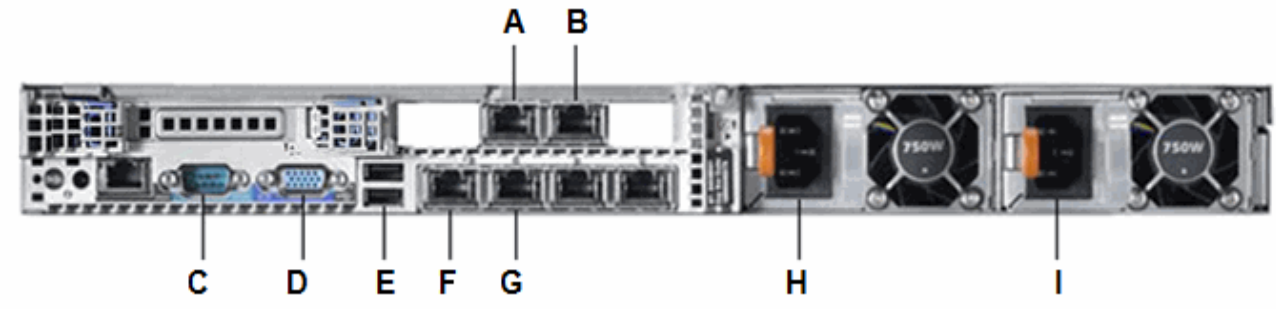
The following table provides the callout details for the front panel.

Table 48: DDoS Secure 1200 FAILSAFE Front Panel Details

CALLOUT	DESCRIPTION
A	Power ON/OFF Button

Figure 2 displays the rear panel for DDoS Secure1200 Failsafe.

Figure 2: Rear Panel



Copyright © 2013, Juniper Networks, Inc

The following table provides the callout details for the rear panel.

Table 49: DDoS Secure 1200 FAILSAFE Rear Panel Details

CALLOUT	DESCRIPTION
A	I-IF (1/10 Gbit Internet Interface)
B	P-I/F (1/10 Gbit Protected Interface)
C	Serial Interface
D	Video (Optional)
E	Keyboard + Mouse (Optional)
F	M-I/F+ILO (1 Gbit Management Interface and Integrated Lights Out)
G	D-IF (Optional 1 Gbit Data Share Interface)
H	Power Supply
I	Power Supply

Copyright © 2013, Juniper Networks, Inc

APPENDIX F

TROUBLESHOOTING

1. My browser gives an SSL connection error

   If the DDoS Secure appliance SSL certificate changes for whatever reason, some PC Browsers choke on the previously installed certificate. If so, the old certificate will have to be removed by hand from the Browser Root Certificate cache. It is possible that exiting the browser and re-connecting fixes the situation.

2. How do I recover my lost Username and Password?

   You are unable to recover the Username and Password. If DDoS Secure appliance is able to access your appliance, they are able to reset the password. It may be that you have to re-image the system.

3. What does **Init Phase xxx** mean?

   When the appliance starts up, various large data sets have to be initialized. Each phase is the initialization of a different data set.

4. What does **Exit Phase xxx** mean?

   When the appliance closes down, various large data sets have to be cleanly closed down. Each phase is the cleanup of a different data set.

5. Why do I get **Protected IP Table Full** turning to red?

   The appliance is set up to protect a maximum number of protected IPs (see license key information for the precise number). If this limit is exceeded, then **protected IP Table Full** will turn to red. If your **I-I/F** and **P-I/F** connectors are reversed, the appliance is effectively protecting the Internet from your internal users. Confirm this using the **PROTECTED INFO** button. Correct any cabling errors. Review the location of the appliance in your network topology if the appliance has to protect more than the specified number of protected IPs. If cabling arrangements are logically reversed without physical disconnection, the DDoS Secure appliance engine must be restarted to ensure the correct automatic re-learning of the network topology. It is also possible to swap the Interfaces with **CONFIGURE INTERFACES**.

Copyright © 2013, Juniper Networks, Inc

APPENDIX G

GUI BRANDING

It is possible to customize both the GUI initial login landing page, as well as the format / style of pages that a portal user may be visiting.

Login Page

It is possible to customize this page by modifying the file customer.tmpl from the Manuals CD. The file has to be named customer.tmpl or host_uri-customer.tmpl, where host_uri is the name or IP that a user uses to access the DDoS Secure appliance.

- customer.tmpl is preserved across software upgrades.
- customer.tmpl can have reference to urls of external sites.
- customer.tmpl can reference existing image files, or portal- specific images.
- customer.tmpl must link to webviewcheck.wsp to enter the DDoS Secure appliance portal.

If the site is accessed with the URL https://some.host.com, then the search sequence is some.host.com-customer.tmpl, then customer.tmpl, and finally the original login page.

Images / CSS files

Once a user has been logged in, they are then associated with a portal. Any .css file in the /css directory, or any images in the /images directory can be customized to modify the output.

Assume that a user is logged into portal CustomerX and is requesting css/center_pane.css. The search order would be css/portal-CustomerX-center_pane.css, then css/portal-center_pane.css and finally css/center_pane.css. The same is true for any images.

Updating Customized Files

To upload the files, on a Linux server, you need to collect all the customized files into a directory, and then running the following linux command to create an update package:-

- echo **w.x.y** > DDoS Secure appliance- ; rm –f portal-clean ; tar cvf files.upg \ DDoS Secure appliance- *customer.tmpl patch-*.

  where w.x.y is the current version of the DDoS Secure appliance (e.g. 4.0.2), and then upload files.upg as a DDoS Secure appliance patch.

Removing Customized Files

Run the following linux command to create an update package:-

- echo **w.x.y** > DDoS Secure appliance- ; touch portal-clean ; tar cvf clean.upg \DDoS Secure appliance- portal-clean

  where w.x.y is the current version of the DDoS Secure appliance (e.g. 4.0.2), and then upload clean.upg as a DDoS Secure appliance patc

Copyright © 2013, Juniper Networks, Inc